InstantScan
使用手册

利基网络股份有限公司
Secure Networks at Layer-7

版权

InstantScan 使用手册

版本 3.0

September 29, 2008

商标

技术支持

利基网络尽可能提供详细的档以供您安装与设定您所购买的InstantScan产品。这些文件能帮助您暸解本产品的功能与设定步骤。您亦可从利基网络网页http://www.L7-Networks.com下载相关产品的文件与数据。

如果您对InstantScan产品有任何技术上的问题或建议，请洽询利基网络技术支持中心。当您洽询技术支持的同时，请您务必准备好以下信息，以节省您与技术人员沟通的时间：

- 产品型号与序号
- 保固期间
- 您收到本产品的日期
- 简述产品的问题与您曾尝试解决的步骤

聯絡方法 / 位置	电子邮件	电话 传真	住址
台湾台北	FAE@L7-Networks.com	+886-2-27936053	台北市新湖三路289号3楼 3F, No. 289, Sinhu 3rd Rd., Neihu District, Taipei City 11494, Taiwan
台湾新竹	FAE@L7-Networks.com	+886-3-5225946	新竹科学工业园区园区二路20号1楼 1F,No.20, Park Ave. II Rd., Science-based Park, Hsinchu, Taiwan 300
中国上海	FAE@L7-Networks.com	+86-21-52185699 +86-21-62386778	上海市北渔路28弄22号701室
中国广州	FAE@L7-Networks.com	+86-20-33820297*11 +86-20-3382-0297*18	广州市天河区天阳路154号太阳广场19D 19D, #154 TianYang Road, TianHe Dist,Guangzhou,China.
日本东京	FAE@L7-Networks.com	+81-3-5434-9678 +81-3-5434-9686	Alphasolutions Co., Ltd. 10F 8-8-5 Nishigotanda, Shinagawa-ku, Tokyo 141-0031, Japan
美国 Santa Clara	FAE@L7-Networks.com	+1-408-844-8850 +1-408-844-8841	Alpha Networks Inc. 3945 Freedom Circle, Suite 1150 Santa Clara, CA 95054, USA

关于本手册

本手册利用 InstantScan内建的网页接口（WBI）画面说明，引导您设定并管理 InstantScan。为了帮助您了解如何使用本产品，您必须先了解 WBI 的使用方法。

对象

本手册尽可能提供您设定 InstantScan 设备的详细信息。其主要指导对象为设定 InstantScan、监控网络安全状态、决定内容管理、与收发报表的网管人员。

相关档

- InstantScan CD
  参考 CD 内附的文件数据。
- 快速安装指南
  快速安装指南协助您快速并且正确地安装硬件与软件。
- 在线协助
  在线协助提供个别的窗口说明与补充数据。
- 利基网络网页
  请参考利基网络网页 http://www.L7-Networks.com 的支援档。

连络讯息

本手册内所提供的设定方法皆已经过测试与验证，如果您发现某些功能已更改（或者发现任何错误），您可以将您发现的错误与您对将来版本的建议邮寄到以下的住址：

300 新竹科学工业园区园区二路 20 号 1楼

+886-3-6668896（电话）

+886-3-6668895（传真）

您可利用电子邮件将讯息传送给我们。如果您想让本公司将您的电子邮件列入本公司邮件列表中或索取产品目录，请寄email到下列电子邮件信箱：

service@L7-Networks.com

寻求技术支持或对本手册有任何评论，请寄到下列电子邮件信箱：

FAE@L7-Networks.com

寻求更近一步有关本手册与本公司产品的信息，请参观本公司网站：

http://www.L7-Networks.com

目录

版权 i
技术支持 ii
关于本手册 iii
第 1 部 产品简介 2
版本快讯 3.0.04 3
第 1 章 产品简介 4
1.1 产品包装检查 4
1.2 硬件安装 4
1.3 将 InstantScan 连上网络 5
1.4 InstantScan 的系统默认值 vs 范例设定 5
第 2 部 基本设定 6
第 2 章 管理服务器安装 7
2.1 管理服务器软件安装 7
2.1.1 管理服务器系统需求 7
2.1.2 软件安装程序 7
2.1.3 客户端安装 8
2.2 设定 InstantScan 8
2.2.1 启动系统 8
2.2.2 系统架构 8
2.2.3 系统参数设定 9
2.2.4 InstantScan 网页接口设定 10
第 3 章 mailer 20
3.1 Mailer 概述 20
3.2 Mailer 设定 20
第 4 章 IM 账号验证 25
4.1 验证的种类 25
4.2 设定验证类型 25
4.2.1 Pop3（s）设定 25
4.2.2 Imap（s）设定 26
4.2.3 Radius 设定 26
4.2.4 LDAP 设定 27
第 3 部 InstantScan 管理系统概述 28
第 5 章 InstantScan 管理系统介绍 29
5.1 InstantScan 技术应用 29
5.2 内容管理流程 31
5.3 InstantScan 网页接口设计原则 31
5.4 InstantScan 图示说明 32
5.5 工具栏说明 33

5.6 管理服务器版本 33
第 6 章 阶层式管理与稽核 34
6.1 需求 34
6.2 目的 34
6.3 方法 34
6.4 步骤 34
6.4.1 新增使用者账号 34
6.4.2 修改用户登入网页接口的密码 37
第 4 部 网络监看 38
第 7 章 网络监看 39
7.1 监看公司网络 39
第 5 部 对象管理员 40
第 8 章 对象管理员 – IP 与 Schedule 41
8.1 需求 41
8.2 方法 41
8.3 步骤 41
8.3.1 地址设定 42
8.3.2 排程设定 44
第 6 部 流量管理员、应用层防火墙 49
第 9 章 流量管理员 50
9.1 需求 50
9.2 方法 51
9.3 步骤 52
第 10 章 应用层防火墙 54
10.1 应用防火墙介绍 54
10.2 需求 54
10.3 方法 54
10.4 步骤 54
10.4.1 设定实时通讯软件规则 55
10.4.2 设定点对点传输软件规则 58
10.4.3 设定 VoIP 规则 60
10.4.4 拦阻 VoIP - Skype File Transfer 62
第 7 部 实时通讯管理员 64
第 11 章 自定义警告讯息 65
11.1 需求 65
11.2 方法 65
11.3 步骤 65
11.3.1 实时通讯服务 65
11.3.2 实时通讯聊天对象 65
11.3.3 实时通讯内容 66
11.3.4 实时通讯病毒防护 66

11.3.5 其余加密软件 67
第 12 章 实时通讯服务/群组 68
12.1 需求 68
12.2 方法 68
12.3 步骤 68
12.3.1 实时通讯服务 68
12.3.2 实时通讯群组 70
第 13 章 实时通讯用户设定 72
13.1 需求 72
13.2 方法 72
13.3 步骤 72
13.3.1 AD Import – Open LDAP 72
13.3.2 AD Import － ActiveDirectory 74
13.3.3 使用 AD Book Import 76
13.3.4 从本地端档案加载实时通讯用户与其群组 78
13.3.5 手动编辑实时通讯用户 81
13.3.6 自动学习实时通讯用户名单 83
13.3.7 从本地端档案导出实时通讯用户与其群组 85
13.3.8 实时通讯用户设定辅助工具栏 86
第 14 章 管理实时通讯用户 87
14.1 需求 87
14.2 方法 87
14.3 步骤 87
14.3.1 新增的实时通讯用户默认值 87
14.3.2 实时通讯用户管理 88
14.3.3 实时通讯聊天对象管理 90
14.3.4 实时通讯内容过滤 91
14.3.5 实时通讯安全防护 96
14.3.6 除外来源端设定 97
第 15 章 LDAP (ActiveDirctory) Import 设定范例 98
15.1 设定 LDAP Browser 软件 98
15.2 设定 LDAP Import – 基本设定 102
15.3 设定 LDAP Import – 进阶设定 103
15.4 LDAP 汇入疑难解答 104
第 16 章 封装管理员 105
16.1 需求 105
16.2 方法 105
16.3 步骤 105
16.3.1 启动封装管理员 105
步骤 1 开启封装管理员 105
步骤 2 上传配置文件 105

第 8 部 网页管理员 106
第 17 章 网页管理员 107
17.1 需求 107
17.2 目的 108
17.3 方法 108
17.4 步骤 109
第 9 部 报表系统 112
第 18 章 报表系统简介 113
18.1 InstantScan 报表系统 113
18.2 报表设计原则 113
18.2.1 报表类别 113
18.2.2 搜寻工具 113
第 19 章 应用层防火墙报表 117
19.1 需求 117
19.2 方法 117
19.3 步骤 117
19.3.1 功能面报表浏览 117
19.3.2 政策面报表浏览 118
19.3.3 个人面报表浏览 119
19.3.4 导出事件报表 121
第 20 章 实时通讯管理员报表 124
20.1 需求 124
20.2 方法 124
20.3 步骤 124
20.3.1 功能面报表浏览 124
20.3.2 政策面报表浏览 126
20.3.3 个人面报表浏览 128
20.3.4 导出事件报表 130
第 21 章 网页管理员报表 133
21.1 需求 133
21.2 方法 133
21.3 步骤 133
21.3.1 功能面报表浏览 133
21.3.2 政策面报表浏览 135
21.3.3 个人面报表浏览 137
21.3.4 导出事件报表 139
第 22 章 流量管理员报表 142
22.1 需求 142
22.2 方法 142
22.3 步骤 142
22.3.1 带宽面报表浏览 142

22.3.2 功能面报表浏览 143
22.3.3 政策面报表浏览 144
22.3.4 个人面报表浏览 146
第 10 部 侧录稽核 149
第 23 章 侧录稽核 150
23.1 需求 150
23.2 方法 150
23.3 步骤 150
23.3.1 实时通讯内容侧录 150
23.3.2 网页内容侧录 151
第 11 部 系统维护 153
第 24 章 系统记录 154
24.1 需求 154
24.2 目的 154
24.3 方法 154
24.4 步骤 154
24.4.1 系统记录 154
24.4.2 设定接收系统记录的时间 155
24.4.3 启用实时接收系统记录 156
第 25 章 系统维护 157
25.1 需求 157
25.2 透过 TFTP 服务器升级韧体 157
25.3 备份配置文件 158
25.4 还原配置文件 159
25.5 启用选购的模块 159
25.6 升级 IM 引擎 / 应用程序行为 / 病毒数据库 / URL 数据库 160
25.6.1 自动升级 IM 引擎 / 应用程序行为 / 病毒数据库 / URL 数据库 160
25.6.2 手动升级应用程序行为 162
25.6.3 手动升级 URL 数据库 163
25.6.4 在 CLI 标准模式下，恢复出厂默认值 163
25.6.5 在 CLI 救援模式下，回复出厂默认值 163
25.6.6 SNMP 控制设定 164
附录 165
附錄 A 指令行接口（CLI） 166
A.1 CLI 指令列表 - 标准模式 166
A.2 CLI 指令列表 - 救援模式 169
附錄 B 疑难解答 171
附錄 C InstantScan 配置图暨相关设定调整建议 173
附錄 D 系统记录语法 179
附錄 E 词汇集 183
附錄 F 索引 187

第1部

产品简介

版本快讯 3.0.04

本节叙述和之前的版本比较起来，本版新增或改善的产品功能。包含InstantScan的操作方式改变、因InstnatScan产品引擎效能与精确性的改善而造成的网页设定接口变更。与上一版比较，2.2.05版提供下列加强功能：

Release 3.0.04 (2008/09/24)

1. [BugFix] Incomplete MSN file recording.
2. [BugFix] Incorrect bandwidth accounting for bridge in CLI and UI (System Status).
3. [BugFix] Auto-reboot due to low memory during firmware upgrade?may cause corrupted flash.
4. [BugFix] Bypass card always goes into bypass since 3.0.
5. [BugFix] Web manager runs in sniffer mode by default.
6. [BugFix] URL keyword blocking now works in partial-matching mode.
7. [BugFix] Blocking policy in L7 must rely on enabling Traffic Manager.
8. [BugFix] No Game/Stock patterns shown in InstantScan series models.
9. [BugFix] UserConsole --> Group without Web Service
10. [BugFix] L4/L7 Manager will not reload configuration after modifing address objects in Object Manager
11. [NewFeature] Support new traffic discovery: App/Host/Policy views.
12. [NewFeature] Support default interface mapping for IX-5000V/IX-5000VB.
13. [Update] (Pattern) Built-in 2.1.05.326
14. [Update] (URLDB) Built-in 2.1.00.021

Release 3.0.02 (2008/09/08)

1. [BugFix] Bridge learning timeout too long (15 seconds) when plugging the INT/EXT cables.
2. [BugFix] Web Manager may accidentally cause CPU 99%.
3. [BugFix] Logging system may be corrupted due to long pattern name.
4. [BugFix] Telnet/Ftp content recording may running out of free memory.
5. [BugFix] AD mapping causes heavy CPU loads at AD server.
6. [BugFix] AD mapping may not work well in Windows 2000 Active Desktop environments.
7. [BugFix] CLI "sys mgtserver" may cause "Invalid Checksum" problems.
8. [BugFix] Session count in AppView is not synchronized with that in HostView.
9. [NewFeature] Support multiple bridge with scheduled Traffic Manager policy rules.
10. [NewFeature] Support manual ordering/naming of network interface for all x86 hardware.
11. [Update] (Pattern) Built-in 2.1.05.320
12. [Update] (URLDB) Built-in 2.1.00.020

第1章 产品简介

本章介绍您如何快速安装 InstantScan。

员工上网不外乎用 Outlook 收信、用 Explorer 浏览网页、用 MSN/Skype 等实时通讯（IM）跟朋友闲聊、用 KaZaA/Kuro/ezPeer 等点对点传输（P2P）下载非法信息。其中，Email 与 IM 是泄密与病毒入侵的管道，而 P2P 更是带宽的杀手与间谍软件的温床。L7 Networks 的 InstantScan 内容管理器，是无惧任何伪装联机的第七层控管设备，以全球领先的 Inline 架构，依时间区段控管、侧录每个员工 IM/P2P 的细部使用行为、聊天对象、传文件档案型别、聊天内容关键词、使用带宽、传档扫毒、蠕虫散布等，并具备强大 IM/P2P 报表系统。除能追踪员工泄密行为/工作绩效/侧录采证外，更对目前 Layer-4 埠号已无法反应实际流量带宽的情况，提供了绝佳的带宽管理与报表系统。

1.1 产品包装检查

请检查您所购买的 InstantScan 产品包装内容，如有遗失，请联络您当初购买本产品的经销商。

编号	品名	备注
1.	设备	
2.	L型固定铁片	
3.	螺丝组	
4.	网络线 （RJ-45）	“串线” x 1
5.	AC 电源线	
6.	RS-232 console 线	
7.	CD	

表格 1-1 产品包装项目

1.2 硬件安装

InstantScan 设备可以固定在标准 19 吋机架上，亦可以独立放置于桌面上。请利用包装盒内附的螺丝组将 L 型固定铁片锁于 InstantScan 上，然后将 InstantScan 安装于机架上。

请依以下核对列表检查您的网络联机是否已经备妥：

1. **InstantScan 设备**
2. **网络设备** – 如路由器、交换器、集线器（Hub）等。
   如果您将 InstantScan 链接到上述网络设备，请使用串线（through）相连。
3. **客户端设备（CPE）** – 如桌上型 PC 或笔记本电脑等。
   如果您将 InstantScan 连结到上述客户端设备，请使用跳线（cross-over）相连。
4. **将 InstantScan RJ-45 端口链接相对应之网络线**

InstantScan 系列产品的硬件规格根据您所购买的型号而有不同。当您将 InstantScan 安装于路由器后方时，所有进出流量皆会受其控管。LAN 端的流量必须连接于 InstantScan Internal 端，而所有连外的流量必须藉由 InstantScan External 端与存取路由器（access router）相连。

1.3 将 InstantScan 连上网络

1. **电源**。首先将电源接上 InstantScan 背面的电源孔，然后将另一端接上电源插座。并将开关切换至 I。请稍候约两分钟，InstantScan 开机完毕后，再进行下一步连接动作。注意，IS-10 只需将变压器的接头接上其背后的电源孔即可启动电源。
2. **Console 界面**。利用 RS-232 console 线，将 InstantScan console 埠与您用来设定 InstantScan 的 PC 对接。您即可透过 CLI 指令来设定 InstantScan 的系统参数。
3. **MGMT 界面**。此管理接口系用来传送 InstantScan 的配置文件封包，所以必须透过网络线与 LAN 端的交换器或集线器相连，且要与管理服务器在同一网段底下。
4. **Internal 界面**。此接口系透过网络线与您位于 LAN 端的交换器或集线器相连，用来管理所有内部可控管的网络流量。
5. **External 界面**。此接口系透过网络线将其与存取路由器相连，用来与因特网联机。
6. **HA 界面**。用来连接备份设备，以确保网络不因硬件或意外而中断。
7. **重设键**。用来重开机用，避免经常开关电源，而缩短软硬件使用寿命。

1.4 InstantScan 的系统默认值 vs 范例设定

在下表中您可比较出厂默认值与本手册范例中所使用的 IP 设定值。请记得，INT （Internal） 端口与 EXT （External） 端口并不需要设定任何 IP。因为 Internal 端口是连接所有 LAN 端受 InstantScan 控管的客户端，而 External 端口为连接对外的网络。端口排列顺序依您所购买的型号而有不同，当您首次使用 InstantScan 时，请进入 CLI 接口查看端口的排列顺序。在权限模式中输入 “ip show”，您可以看出所有依照端口编号排列的端口，然后对照您设备上的编号，即可以此顺序来链接您的网络线。

项目		预设设定	范例设定
Password		admin	admin
Internal	Port No.	1	N/A
	IP Address	N/A	N/A
	Subnet mask	N/A	N/A
	Status	DOWN	UP
External	Port No.	2	N/A
	IP Address	N/A	N/A
	Netmask	N/A	N/A
	Status	DOWN	N/A
MGT	Port No.	3	3
	IP Address	192.168.1.1	192.168.168.201
	Netmask	255.255.255.0	255.255.255.0
	Gateway IP	192.168.1.254	192.168.168.254
	Primary DNS	0.0.0.0	168.95.1.1
	Secondary DNS	0.0.0.0	0.0.0.0
	Status	DOWN	UP
HA	Port No.	4	4
	IP Address	N/A	N/A
	Netmask	N/A	N/A
	Status	DOWN	DOWN
Management Server	IP Address	尚未设定	10.1.1.10
	Subnet mask	尚未设定	255.255.255.0
	Gateway IP	尚未设定	10.1.1.254
	Primary DNS	尚未设定	168.95.1.1
	Secondary DNS	尚未设定	N/A

表格 1-2 InstantScan 相关系统默认值

第2部

基本设定

第2章
管理服务器安装

本章节介绍管理服务器的软件安装与网络设定

2.1 管理服务器软件安装

2.1.1 管理服务器系统需求

- ✓ 操作系统 （OS） 至少应为 Windows 2000/2003、Windows XP 或更高等级。如果您的操作系统为英文板，请先安装繁体中文字型套件，否则无法正常显示中文字型。语言套件安装窗口将于您开始安装管理服务器时显示，请点选 Install 安装。



图表 2-1 语言套件安装画面

- ✓ 硬盘至少 80GB 以上可使用空间，建议最好有 120GB 可使用空间。
- ✓ CPU 最少是 Pentium 4 或同等级。
- ✓ 内存最少 256MB，建议最好 512MB 以上。
- ✓ 如果您的操作系统是 Windows XP service pack 2，且启用其内建的防火墙，请记得依以下步骤开启端口 514、1080 和 3306。如此一来，所有封包的进出，才不会因防火墙的拦阻而有所漏失，管理服务器才会正常运作。
  1. 到开始 > 设定 > 网络联机。
  2. 点选区域联机，按鼠标右键选择内容。
  3. 到进阶 > 设定值 > 例外。点击新增端口...
  4. 输入名称与端口编号，点选此端口所使用的通讯协议（UDP 或 TCP）。点击**确定**储存设定值。

名称	端口编码	通讯协议
Log Server	514	UDP
Socks	1080	TCP
Database Server	3306	TCP

表格 2-1 管理服务器端口设定

2.1.2 软件安装程序

1. 安装 Management Server
2. 安装 AD Log Server
3. Management Server 版本升级

4. 浏览光盘
5. 反安装全部(只限移除 Management Server)
6. 反安装 AD Log Server
7. 离开安装接口

⚠ 注意：

1. 当您重新安装管理服务器，或升级管理服务器，请记得重新启动计算机，系统才会运作正常。详细的安装说明，请参考快速安装指南。
2. 如果您曾经安装过 MySQL 与 Apache 任何的版本，妳必须移除您所安装的 MySQL 与 Apache 软件，请参考附录说明。

2.1.3 客户端安装

在您安装好 InstantScan 管理服务器并将 InstantScan 上的网络线链接完成后，您即可利用网页浏览器，在网址列上键入 http://<管理服务器 IP 地址>/ 来连上管理服务器。当您第一次透过浏览器连上管理服务器时，Java Plug-in 将从管理服务器端安装到您的客户端计算机上。

⚠ **注意：**客户端在第一次透过浏览器连上管理服务器时，因浏览器的因素，必须花几分钟时间安装 Java plug-in 程序，请耐心等候。

2.2 设定 InstantScan

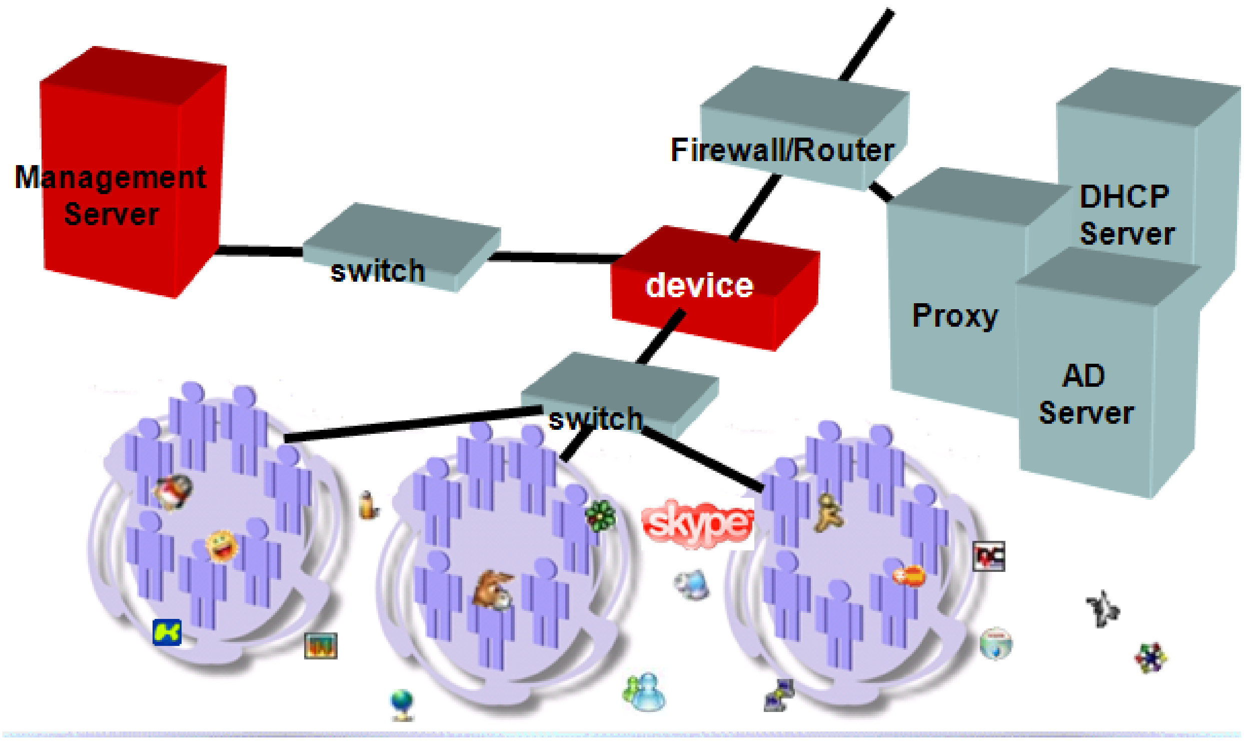
在您开始控管 InstantScan 设备前，请先利用 InstantScan 的 console 接口，直接用 RS-232 console 线与用来设定 InstantScan 客户端的 PC 对接。然后，透过 CLI 指令来设定 InstantScan 的系统参数。之后，您可以利用 Telnet、SSH，或其他 terminal 等远程联机方式来更改系统参数。

2.2.1 启动系统

将邻近 InstantScan 电源插槽的电源开关打开。在开机完成后，系统将要求您输入 ID 与密码。此时，默认的 ID 与密码皆是 admin。在登入系统后，您可以利用 CLI 指令更改密码。详细 CLI 指令，请参阅附錄 A 说明。

2.2.2 系统架构

InstantScan以通透模式安装于网络上，不需更改既有的网络架构。InstantScan管理服务器配合InstantScan管理系统与报表系统，提供您简而易用的用户管理接口来设定管理政策。网管人员可根据网络架构与公司政策来订定各式各样的管理政策。一台管理服务器可同时控管多台InstantScan，并且可接收与分析被控管的 InstantScan 之事件记录。您可将管理服务器安置于任何网络位置。本手册提供一个基础的 InstantScan 网络安装架构。只要您了解基本的安装原理，您即可根据贵公司的网络架构安装您的 InstantScan。



图表 2-2 InstantScan 系统的讯息递送

如**錯誤! 找不到參照來源。** 所示，您必须指定 IP 地址给 **1）InstantScan 管理接口**（Management 端口）；**2）管理服务器**；与 **3）管理端 PC**。InstantScan 可安装于企业网络内部或外部。当网管人员新增一条管理规则，并将设定文件上传，管理服务器立即将配置文件上传至InstantScan。当受到InstantScan控管的PC启用任何实时通讯(IM)软件或点对点(P2P)传输软件时，InstantScan 会将这些事件记录传送给管理服务器储存。管理服务器依您的时程规划，定期产生报表寄送给网管人员分析。

2.2.3 系统参数设定

请用随机内附的 RS-232 console 线，将InstantScan console接口与用来设定InstantScan的PC之串行端口相连，您可选择COM1埠或COM2埠来设定InstantScan。请参考以下超级终端机的设定范例。

终端机类型	超级终端机
每秒传输位	115200
数据位	8
同步检查	无
停止位	1
流量控制	无

表格 2-2 终端机设定

步驟 1 登入系统 系统默认的登入账号密码为 **admin/admin**。之后您可以根据 CLI 指令来更改密码。 **注意!!!** 密码的长度必须藉于5~20字符间。小于5个字符或大于20个字符都会被系统拒绝。相关CLI指令请参考**錯誤! 找不到參照來源。**。	InstantScan login: admin Password: Welcome to InstantScan... InstantScan>

步驟 2 设定InstantScan IP 地址

键入 **en** 进入权限模式。键入 **ip set** 指令来设定MGT 端口的相关 IP 地址。

注意，请先安装好管理服务器，否则系统将回复您" You must make sure the management server works well first."的讯息。

```
Please enter the IP configuration for this device.
  IP Address [192.168.17.93]:
  Netmask [255.255.255.0]:
  Default Gateway [192.168.17.254]:
  Primary DNS [168.95.1.1]:
  Secondary DNS [0.0.0.0]:

  Your configuration is:
  ===========================================================================
  Gateway: 192.168.17.254
  Primary DNS: 168.95.1.1
  Secondary DNS: 0.0.0.0
  Management Server: 192.168.17.205
  ===========================================================================
  Port Interface IP Address        Netmask          Status
  ---- --------- ---------------- ---------------- --------------------------
    1     INT3          N/A              N/A       UP   (Bridge 3)
    2     EXT3          N/A              N/A       UP   (Bridge 3)
    3     MGT     192.168.17.93   255.255.255.0    UP
    4     HA          N/A              N/A         DOWN (HA Disabled)
    5     INT1          N/A              N/A       UP   (Bridge 1)
    6     EXT1          N/A              N/A       UP   (Bridge 1)
    7     INT2          N/A              N/A       UP   (Bridge 2)
    8     EXT2          N/A              N/A       UP   (Bridge 2)
  ===========================================================================
  Do you really want to apply and save [Y/N]? [N]? y
  Waiting for system setting.....
  Setting done.
```

步驟 3 查看目前InstantScan设定状况

键入ip show，您可以看到目前InstantScan的IP设定状况。

```
  ===========================================================================
  Gateway: 192.168.17.254
  Primary DNS: 168.95.1.1
  Secondary DNS: 0.0.0.0
  Management Server: 192.168.17.205
  ===========================================================================
  Port Interface IP Address        Netmask          Status
  ---- --------- ---------------- ---------------- --------------------------
    1     INT3          N/A              N/A       UP   (Bridge 3)
    2     EXT3          N/A              N/A       UP   (Bridge 3)
    3     MGT     192.168.17.93   255.255.255.0    UP
    4     HA          N/A              N/A         DOWN (HA Disabled)
    5     INT1          N/A              N/A       UP   (Bridge 1)
    6     EXT1          N/A              N/A       UP   (Bridge 1)
    7     INT2          N/A              N/A       UP   (Bridge 2)
    8     EXT2          N/A              N/A       UP   (Bridge 2)
  ===========================================================================
```

2.2.4 InstantScan 网页接口设定

InstantScan 管理系统与报表系统使用 Java 平台设计，需要支持 Java Plug-in 程序。所以客户端必须从管理服务器处安装 Java Plug-in，才可浏览管理服务器网页。**当您第一次使用 IE 浏览器连结管理服务器时，Java Plug-in 便会自动安装进您的计算机。第一次登入时需要一些时间让程序初始化，请耐心等候。**

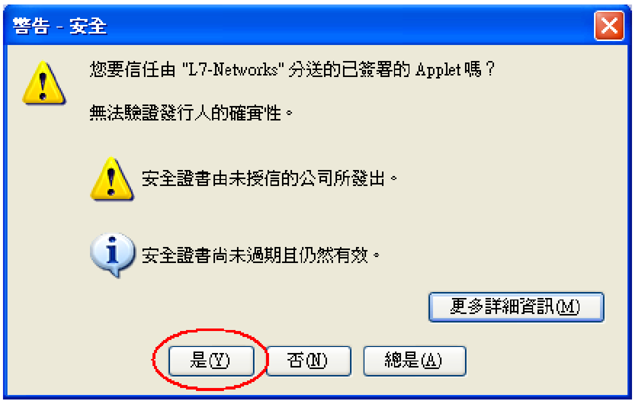
步驟 1 连结管理服务器

指定一组 IP 地址给用来控管 InstantScan 的 PC （例如：192.168.168.1）。打开您的 IE 浏览器，在网址列上键入 http://<管理服务器 IP 地址>。例如，输入 http://10.1.1.10 来连结管理服务器。

注意：如果您的管理端PC、管理服务器、与InstantScan装置不在相同网段内，请记得增加 NAT规则，允许不同网段的封包可以相互传送接收。否则您无法透过管理服务器链接到 InstantScan装置。

步驟 2 安全警告窗口

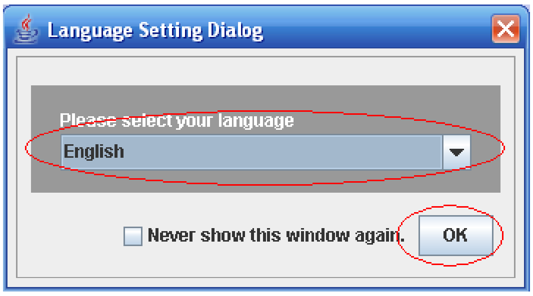
点击**是**接受此验证。如果您不想每次都出现此警告窗口，请点击**总是**。当您点击**是**或者**总是**后，您就可以进入登入画面。



步驟 3 选择语言模块

InstantScan目前提供英文、繁体中文、简体中文等三种语言模块供您选择，您可以选择您喜爱的语言当成网页接口的默认语言模块。点击 OK 进入登入画面。

注意，当进入网页接口后，欲变更语言模块，您可以到 Tools > Language Setting 变更。



步驟 4 登入

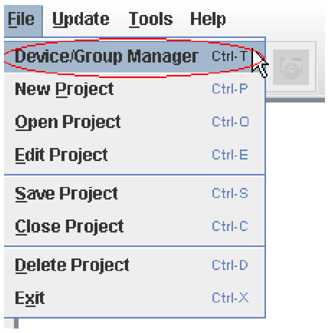
输入ID/Password （预设都是 admin）。确认通过后，即可进入管理页面。

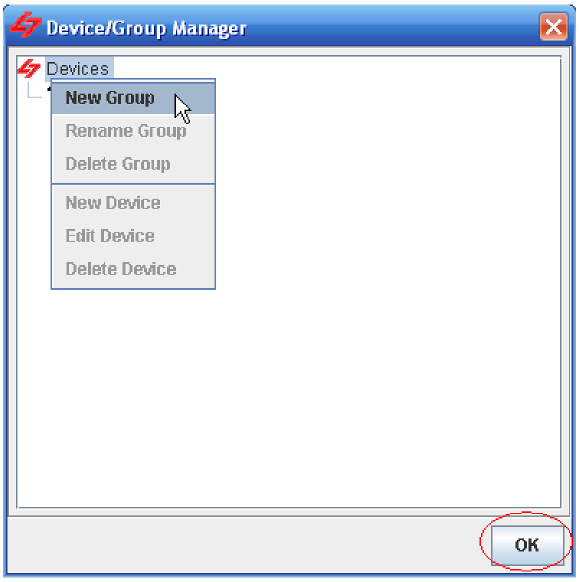
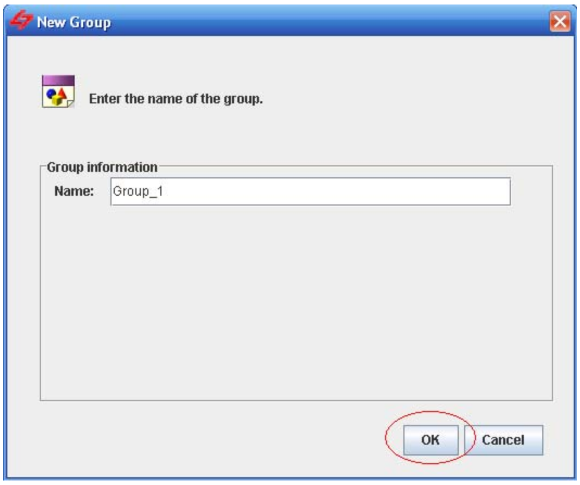
2.2.4.1 建立装置/群组

步驟 1 新增装置/群组

当您成功登入 InstantScan 后，请点选 Device/Group Manager 选项来新增 InstantScan 装置与群组。

File > Device/Group Manager

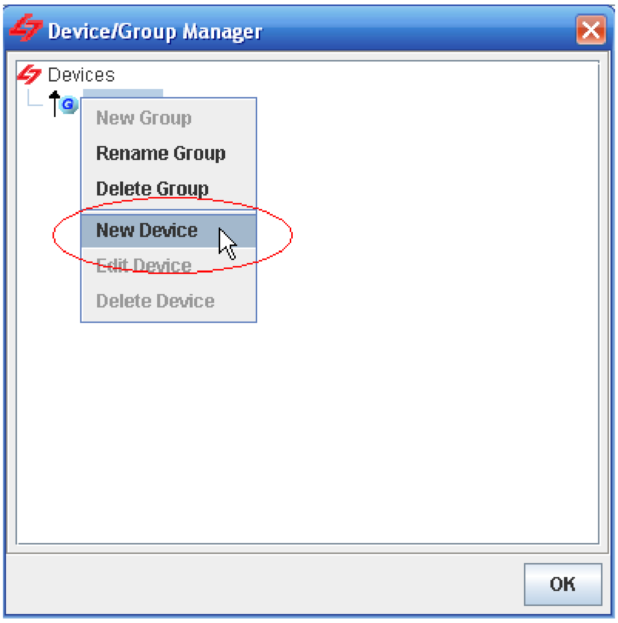


步驟 2　新增群组 在 Devices 上右键单击，然后点选 **New Group**。	**File > Device/Group Manager > New Group** 
步驟 3　输入组名 输入此群组的名称，然后点击 **OK** 继续。之后，组名将显示在屏幕上。您可以右键单击选择 Rename Group 或 Delete Group 来修改或删除此群组。	**File > Device/Group Manager > New Group** 

步驟 4 新增装置

在群组 Group_1 上右键单击，然后点选 New Device。

File > Device/Group Manager > New Device

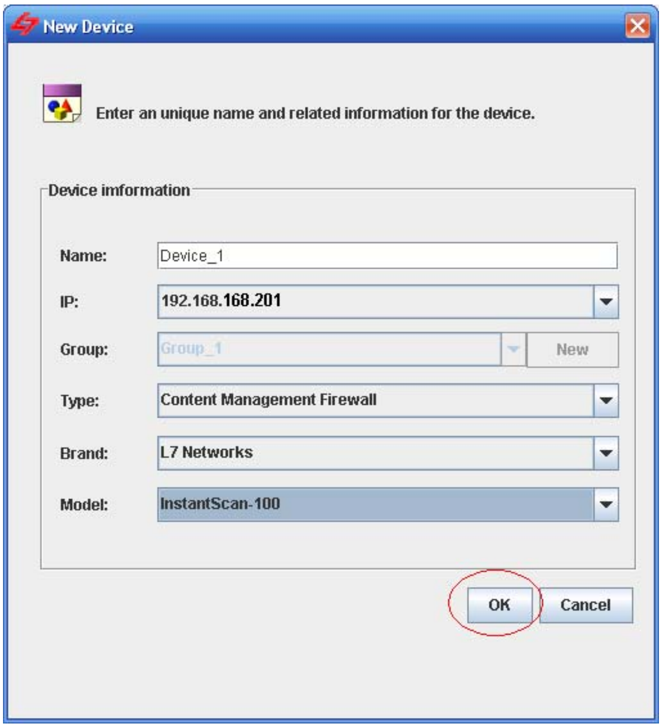


步驟 5 编辑相关装置的信息

输入设备名称，并选择一组已指定其管理服务器的 InstantScan 装置之 IP 地址，然后输入其余相关信息。点击 **OK** 储存设定。

注意：您必须先透过 CLI 接口，设定好装置上的 IP，然后指定管理服务器 IP 地址，否则您无法在 UI 上新增任何装置。当您设定好装置后，管理服务器将自动撷取属于其列管的 device 信息。只要是已经设定过的装置，就不可以再被设定。也就是说，当您已经设定好Device_1 192.168.168.201，如果您要再新增装置时，IP 字段内将不会再出现 192.168.168.201 这个 IP 地址。

File > Device/Group Manager > New Device

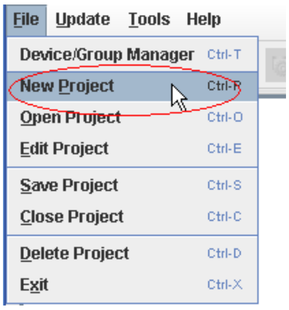


2.2.4.2 新增专案

步驟 1 新增专案

选择 **New Project**。

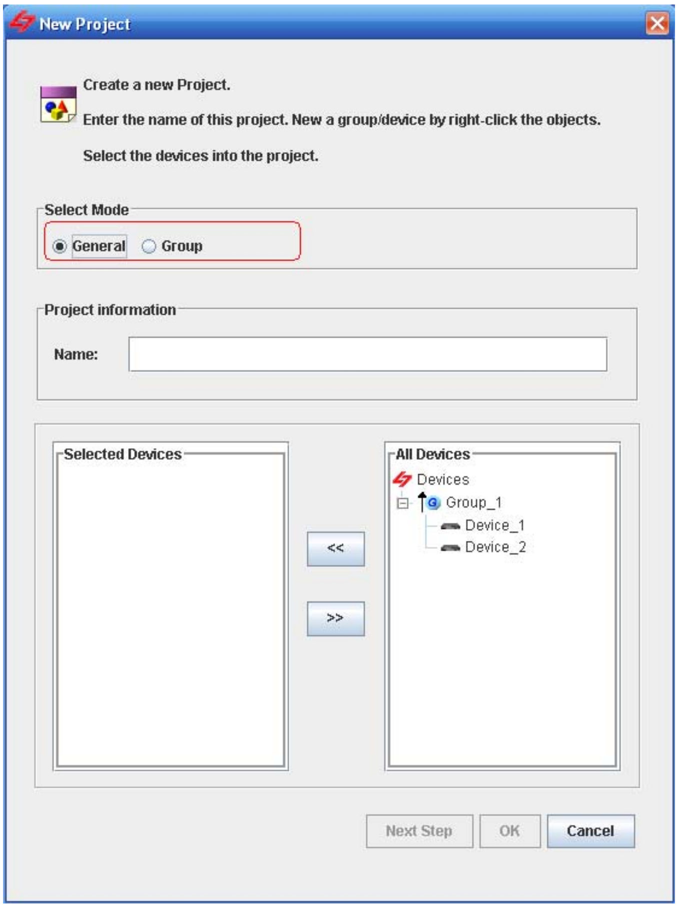
File > New Project



步驟 2 建立新项目

首先，请点选项目的模式，输入项目名称，从 **All Devices** 字段中选择要加入此项目的装置，然后点击 **<<** （左向箭头）将点选的装置加到 Selected Devices 字段。如果您要从此项目移除某个装置，请点选该装置，然后点击 **>>** （右向箭头）即可。

File > New Project > New Project



项目模式	说明
General （一般）。	您希望每台 InstantScan 装置可以拥有其个别的配置文件，每台装置可摆放在不同的网络位置，且各自独立运作，您可以选择此模式。
Group （群组）	当您购买 2 台或 2 台以上 InstantScan 装置，希望简化设定的步骤，所有装置的配置文件共享，其报表系统也共享。也就是说，不管您在哪一台 Device 上变更配置文件，此配置文件都会写进基底装置（Base Device）的配置文件中。其他装置只要重载配置文件即可撷取最新的配置文件。

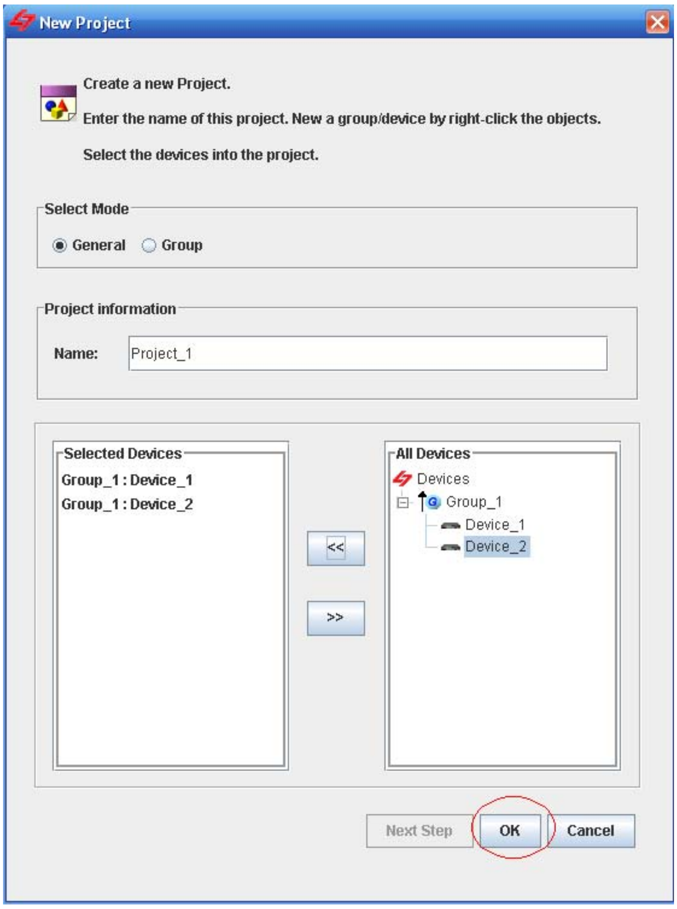
表格 2-3 项目模式

一般项目模式

步驟 1 新增一般项目模式

选择 **General** （一般）为项目的模式，这个模式适合大部分的案例。输入项目名称，从 **All Devices** 字段中选择要加入此项目的装置，然后点击 **<<**（左向箭头）将点选的装置加到 **Selected Devices** 字段。如果您要从此项目移除某个装置，请点选该装置，然后点击 **>>** （右向箭头）即可。最后点击 **OK** 结束设定。

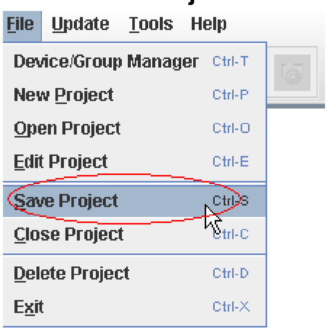
File > New Project



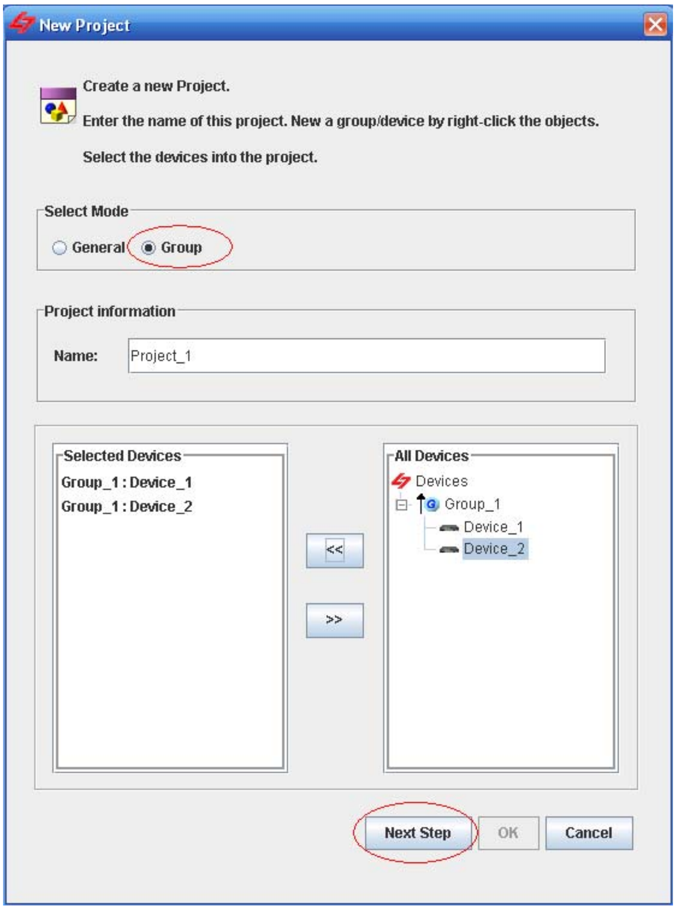
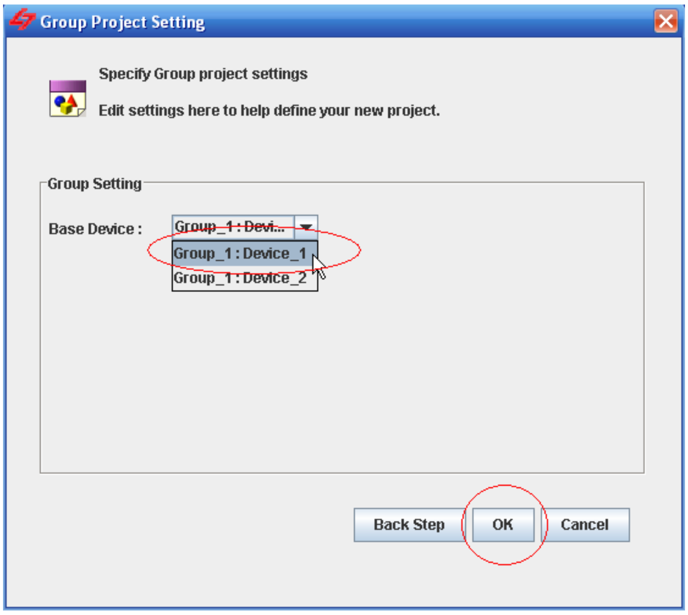
步驟 2 储存项目

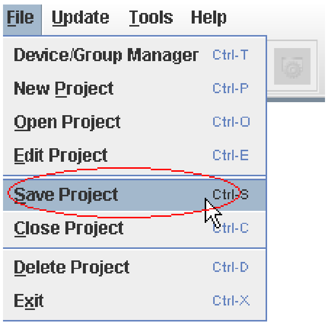
点选 **Save Project** 储存已建立的项目。

File > Save Project

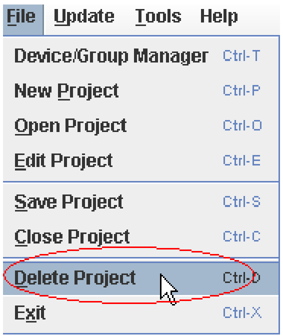


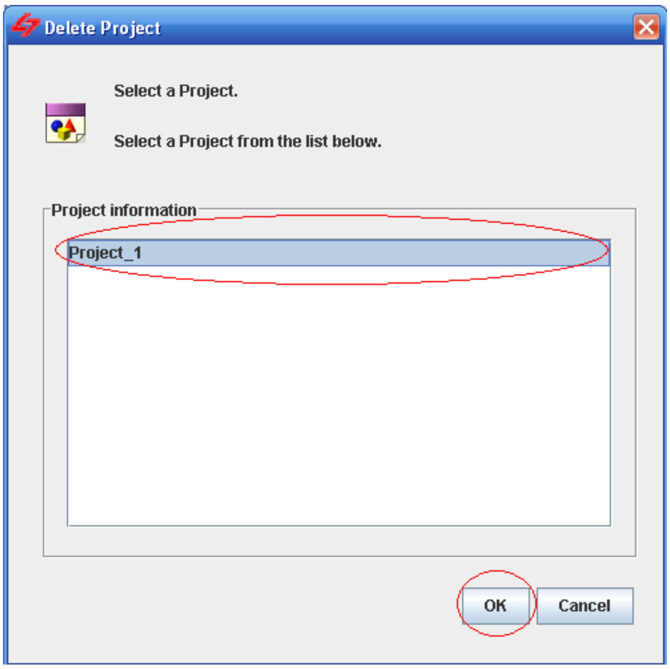
群组项目模式

步驟 1 新增群组项目模式 选择 **Group** （群组）为项目的模式，这个模式适合购买多台 InstantScan，希望简化设定步骤，节省人力资源的公司。输入项目名称，从 **All Devices** 字段中选择要加入此项目的装置，然后点击 **<<**（左向箭头）将点选的装置加到 **Selected Devices** 字段。如果您要从此项目移除某个装置，请点选该装置，然后点击 **>>** （右向箭头） 即可。最后点击 **Next Step** 继续下一步骤。	**File > New Project** 
步驟 2 选择基底装置 选择 **Base Device**（基底装置），当您选择基底装置后，所有此项目内的装置都会读取这个基底装置的配置文件，且读取的报表是所有装置的总和。最后点击 **OK** 结束设定。	**File > New Project > Next Step** 

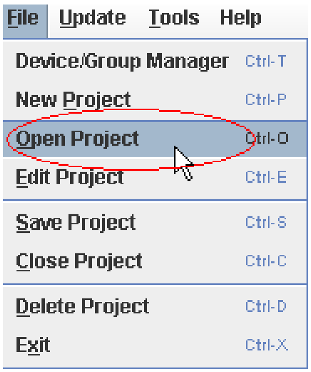
<table>
<tr><td>步驟 3 储存项目
点选 Save Project 储存已建立的项目。</td><td>File > Save Project
</td></tr>
</table>

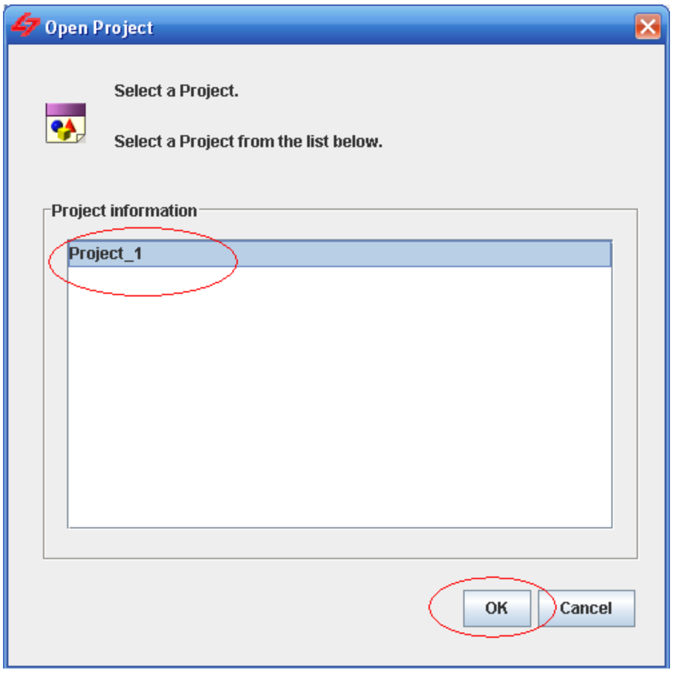
2.2.4.3 删除项目

<table>
<tr><td>步驟 1 点选删除项目
点选 Delete Project 选项。</td><td>File > Delete Project
</td></tr>
<tr><td>步驟 2 删除项目
选择您想删除的项目，然后点击 OK 关闭窗口。

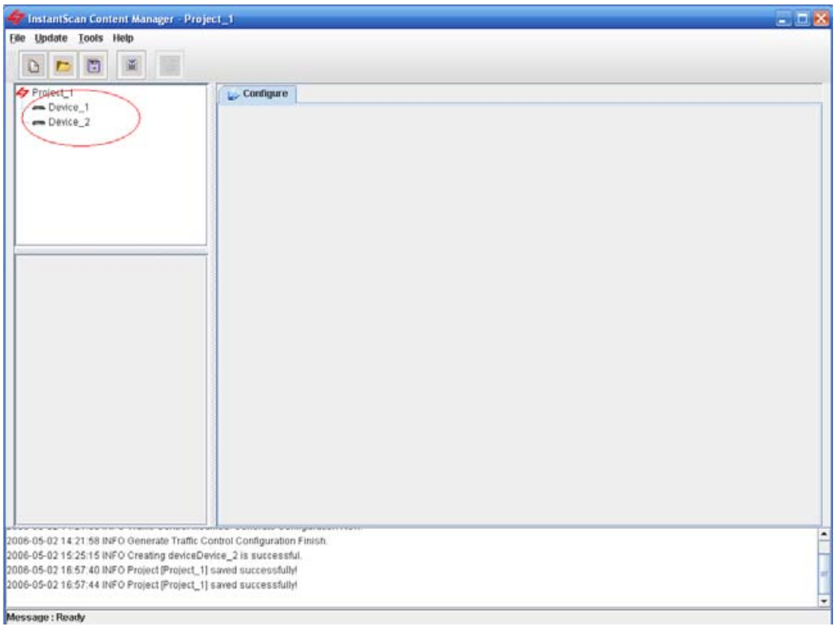
注意：
1. 一旦您点击 OK 按钮后，此项目即刻会从系统中删除。
2. 正在执行中的项目无法删除，您必须先关闭项目，才可选择删除项目。</td><td>File > Delete Project
</td></tr>
</table>

2.2.4.4 开启已存在的项目

<table>
<tr>
<td>步骤 1 开启专案
点选 Open Project 选项。</td>
<td>File > Open Project


</td>
</tr>
<tr>
<td>步骤 2 选择要开启的专案
选择您要开启的专案。点击 OK 关闭窗口。</td>
<td>File > Open Project


</td>
</tr>
</table>

步驟 3 管理 InstantScan	**File > Open Project**
现在，您可以开始管理您的 InstantScan。一个项目可以同时控管多台可能属于不同群组的装置。将鼠标移到您要控管的装置上点两下，系统将链接到此装置，并下载其配置文件。	

第3章
mailer

本章介绍 mailer 的设定与其应用

3.1 Mailer 概述

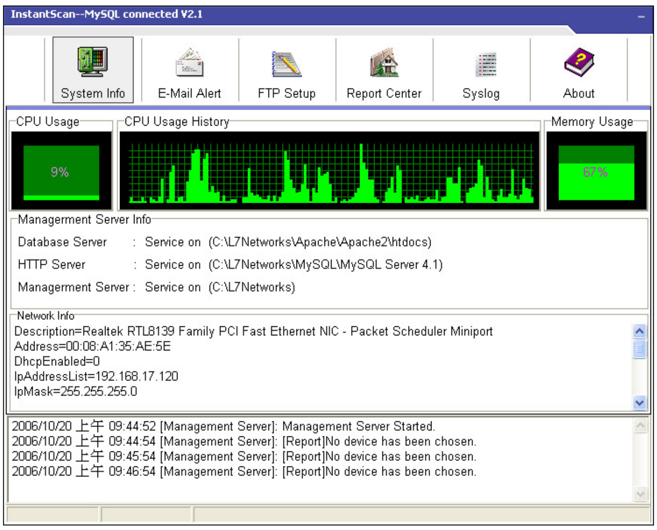
在管理服务器安装完成，且重开机后，有一小图示 （mailer）将会显示在服务器的右下角。请将鼠标移到图标上，点两下。mailer 的功用如下：

- **系统信息**：查询 CPU/Memory 使用状态、数据库/HTTP/管理服务器的存取目录、管理服务器的 IP/MAC 等相关信息。
- **邮件警告**：设定邮寄服务器与自定义电子邮件警告内容。
- **FTP 备份**：设定 FTP 服务器、数据备份时间与备份类型、并选择备份状态。
- **报表中心**：可选择报表寄发的时间、格式、报表收件者与选择报表的来源 (装置)。在设定报表中心前，请在装置上设定导出报表的项目，相关设定请参考章节。
- **系统记录**：设定系统操作记录的收件者，与希望收到的系统记录的严重等级。

详细设定说明，参请考以下的说明。

3.2 Mailer 设定

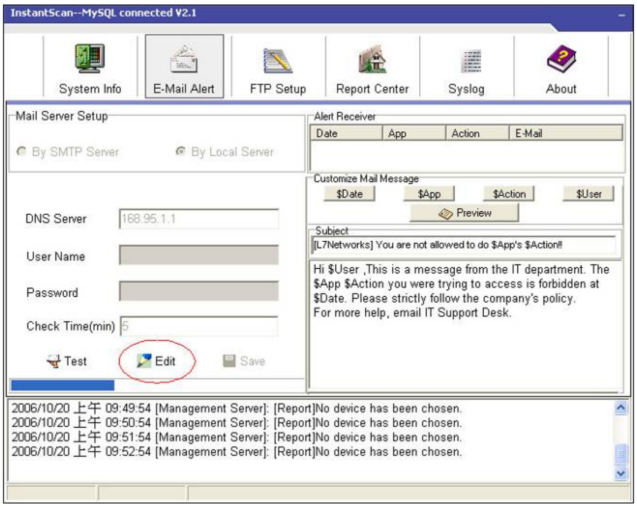
在管理服务器安装完成，且重开机后，有一小图示将会显示在服务器的右下角。请将鼠标移到图标上，点两下。

步驟 1 系统信息	**mailer > System Info**
在这个页面上，您可以看到 CPU 与内存的使用情况，还有一些管理服务器的存放位置、网络讯息等。	

步驟 2 设定邮件服务器

点击 **Edit** 按键。选择 **By Local Server** 选项。输入 DNS 服务器 IP 地址，并在 **Check Time（min）**字段上键入系统检查是否有警告信件的时间。如果您希望透过 SMTP 服务器寄送警告信件，请点选 **By SMTP Server** 选项。您可以点击 **Test**，然后在弹跳出来的窗口内输入收件者的电子邮件地址，最后点击 **OK** ，测试联机状态。

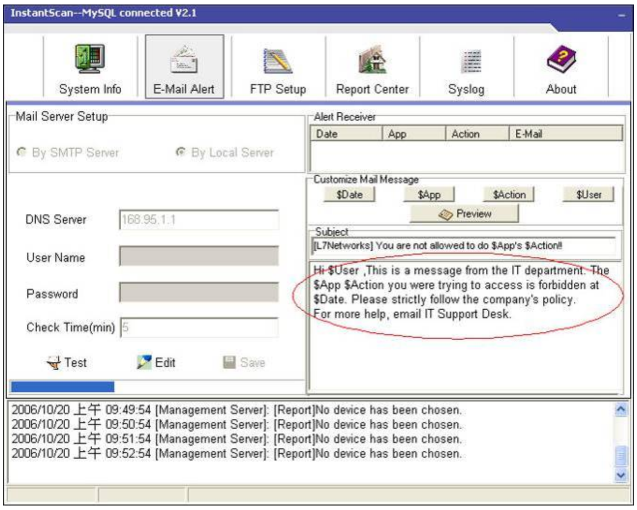
Mailer > E-Mail Alert > Edit



步驟 3 客制化邮件讯息

将光标移到文本框中要加入变量的位置，点击变量（$Date、$App、$Action、$User）。

Mailer > E-Mail Alert > Customize Mail Message



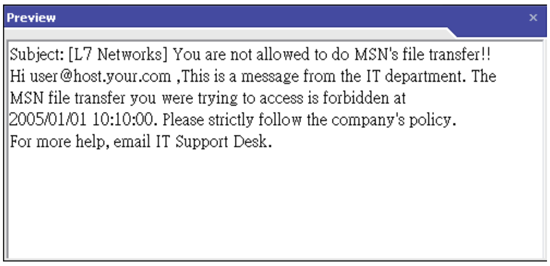
变量名称	说明	范例
$Date （日期）	违反政策事件发生的日期。	2005/01/01 10:10:00
$App （应用软件）	IM用户违反政策时所使用的IM软件。	MSN
$Action （使用行为）	不合法的IM使用行为。	file transfer
$User （使用者账号）	违反政策的IM使用者账号。	user@host.your.com

表格 3-1 警告信件内的变量设定

步驟 4 预览警告邮件内容

当您设定好警告信件内容，可点击 **Preview** 预览。关闭预览窗口继续下一步。

Mailer > E-Mail Alert > Customize Mail > Preview

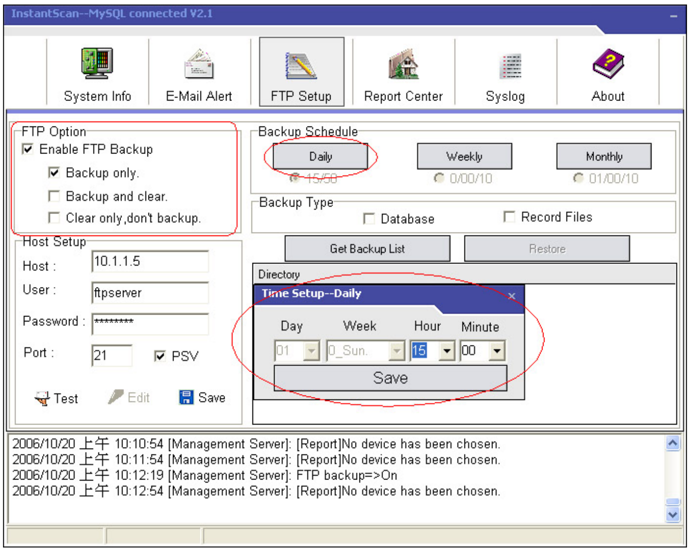


步驟 5 FTP 设定

在本页，您可设定利用FTP备份记录的方式。勾选 **Enable FTP Backup**，然后勾选 **Backup only**。

您可以选择FTP自动备份的时间 1） 每日 2） 每周 3） 每月。点击 **Daily**，然后选择**15 : 00**。换句话说，每天下午 3 点，系统会开始透过 FTP 备份当天的事件记录。

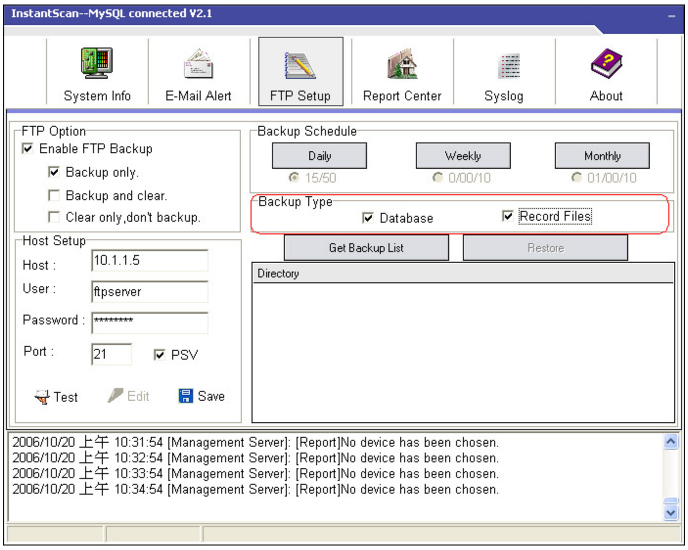
Mailer > FTP Setup > FTP Schedule



步驟 6 设定备份类型

请在 **Backup Type** 选择数据备份类型。当您要还原您已被份的数据，请点击 **Get Bakup List** 按钮，然后选择要从 FTP 服务器上下载的路径，点击 **Restore** 开始数据库或文件还原。

Mailer > FTP Backup > Backup Type

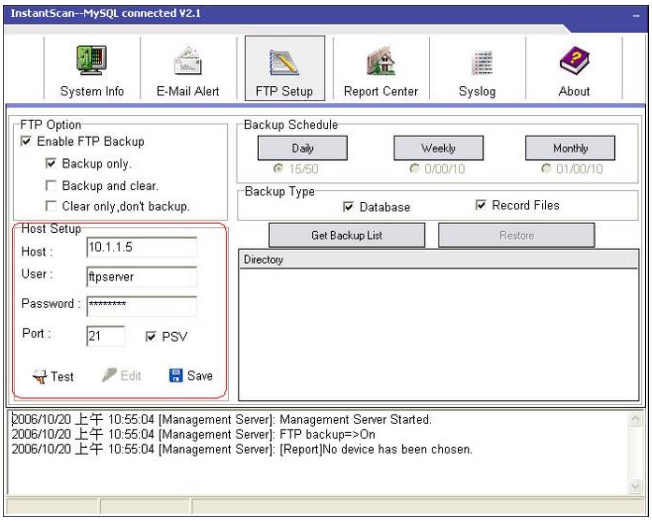


步驟 7 FTP 服务器设定

点选 Edit 开始编辑相关设定，输入 FTP 服务器 IP 地址、用户账号与密码。如果 FTP 服务器使用 passive mode 的话，请勾选 PSV。点击 Test 测试 FTP 联机状况。再点选 Save 记录您所设定的相关选项。

承上所述，您选择每日下午 3 点 00 分备份 log，系统将于此时自动 FTP 备份 log。所备份的文件夹将会以该日的日期命名。

Mailer > FTP Setup > Host Setup

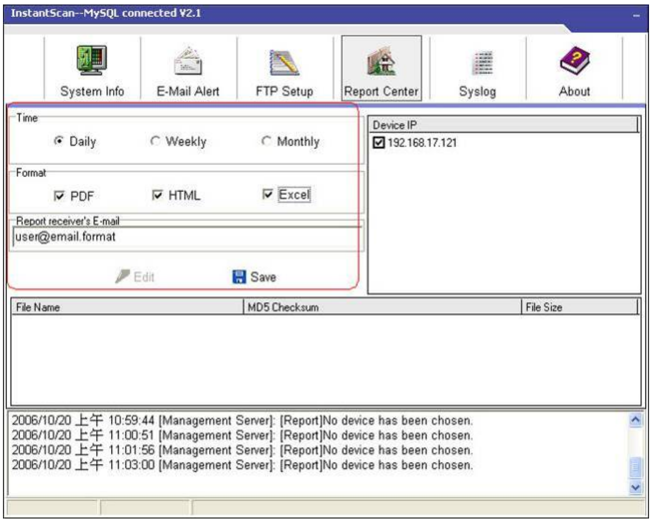


步驟 8 报表中心

点选 Edit 开始编辑相关设定，选择寄送报表的时间（每日 / 每周 / 每月）。勾选您希望收到的报表格式（PDF/HTML/Excel），与勾选希望收到哪些 InstantScan 设备的 log。输入收信者的电子邮件信箱。再点选 Save 记录您所设定的相关选项。

注意：在您设定报表中心前，请先确定您已经在 InstantScan 用户接口上上定好报表输出的项目与格式，否则您收到的报表会是空的。

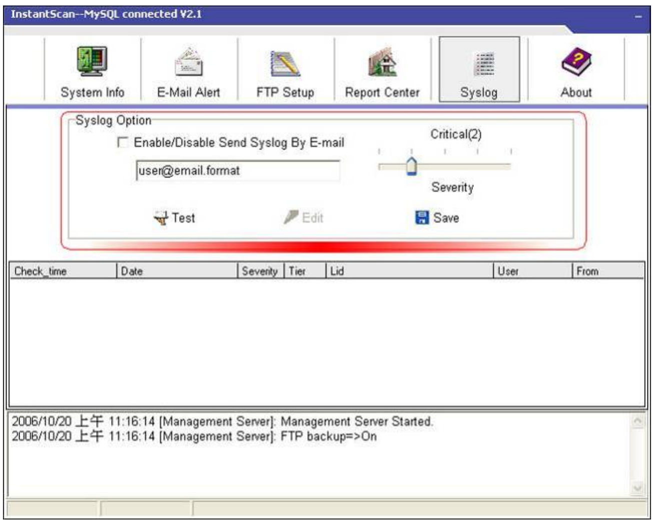
Mailer > Report Center

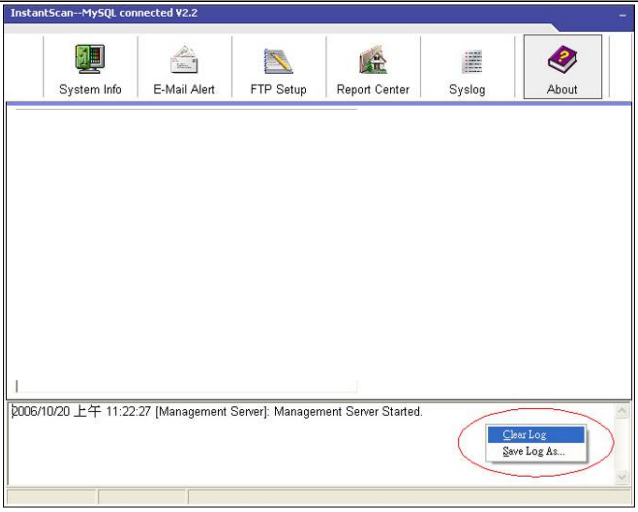


步驟 9 系统记录

点选 Edit 开始编辑相关设定，勾选 Enable/Disable Send Syslog By E-mail，然后在空格处填写您的 Email 地址。利用鼠标移动到您想要收到的系统记录的等级。共分为 5 个等级 1) Alert （警告）2) Critical （严重） 3) Warning （警示） 4) Notification （注意）5) Information（信息）。如果您只希望收到 Alert 等级的系统记录，只要将指针拉到 Alert 的位置。但是，如果您希望收到所有的系统记录，您必须把指针拉到 Information 的位置。点击 Test 测试 E-Mail 信箱。再点选 Save 记录您所设定的相关选项。

Mailer > Syslog



步驟 10 清空/储存系统记录 在状态区内右键单击。您可选择清空事件记录或者将纪录储存到硬盘上。	

如果您不小心关闭 mailer，您可以在桌面或 C 磁槽根目录，L7 Networks 文件夹内找到档案 mailer.exe。移动您的鼠标，在 mailer.exe 图示上点两下，即可开启它。Mailer 默认储存的路径为 C:/L7Network。

第4章
IM 账号验证

本章介绍如何设定 IM 账号验证，让用户透过 InstantScan 注册实时通讯账号。

InstantScan 支持 POP3（s）、IMAP（s）、Radius、LDAP 等账号验证方式。使用者可以您可以结合现有的 POP3（s）、IMAP（s） 邮件系统资源，让通过验证的用户注册自己的实时通讯账号。您亦可以利用 Radius 或 LDAP 服务器让使用者透过向服务器验证通过，取得注册账号的权限。

4.1 验证的种类

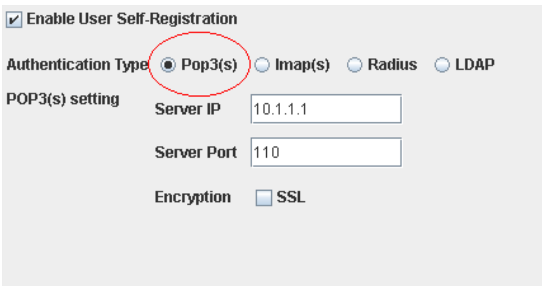
使用者必须透过浏览器完成账号验证。当您设定好验证类型，使用者只要在网址列上键入 InstantScan 设备的 IP 地址，验证的窗口就会显示出来。

请参考下列五个步骤来设定账号验证：

1. 启用验证功能。
2. 设定验证类别。
3. 设定验证各项参数。
4. 透过 IE 浏览器，在网址列上键入 https:// InstantScan IP 地址/ （例如: https://192.168.168.201/） 连结验证网页.

4.2 设定验证类型

4.2.1 Pop3（s）设定

步骤 1 设定 Pop3（s）验证 勾选 **Enable User Self-Registration**（启用验证）。选择 **Pop3（s）**为验证类型。输入服务器 IP 和服务器端口。如果您的服务器需要透过加密（埠号 995）联机验证，请勾选SSL。然后上传配置文件。 **注意:** Pop3 服务透过端口 110 联机而 Pop3s 服务透过端口 995 联机。	**IM Manager > Auth > Pop3（s）** 

字段	说明	范例
Server IP	Pop3（s）服务器的 IP 地址。	10.1.1.1
Server Port	Pop3（s）服务器数据进出的通讯端口。例如，Pop3 服务透过端口 110 联机而 Pop3s 服务透过端口 995 联机。	110
Encryption	所谓的 SSL 是利用大数值编码的技术将数据编码后再传至远程，全球信息网在建置之后，必须向一个有公信力的单位登入，并取得一个 Private Key，而将另一个 Public Key 放在网络上；数据在因特网传输时都是经过编码的数据，即使有人在中间要撷取这些经过编码的数据，看到的都是一些毫不具意	不启用

	义的乱码，这种编码的另一种理论基础是，凡是经过 Public Key 编码过的数据，都必须利用 Private Key 才能解得开。	

表格 4-1 POP3（s）设定

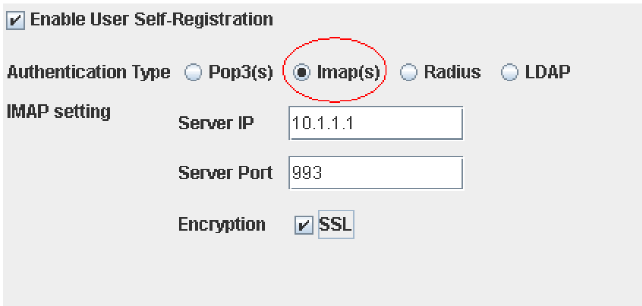
4.2.2 Imap（s）设定

步驟 1 设定 Imap（s）验证

勾选 **Enable User Self-Registration**（启用验证）。选择 Imap（s）为验证类型。输入服务器 IP 和服务器端口。如果您的服务器需要透过加密（埠号 995）联机验证，请勾选SSL。然后上传配置文件。

注意：Imap 服务透过端口 143 联机而 Imaps 服务透过端口 993 联机。

IM Manager > Auth > Imaps（s）



字段	说明	范例
Server IP	IMAP（s）服务器的 IP 地址。	10.1.1.1
Server Port	IMAP（s）服务器数据进出的通讯端口。例如，IMAP 服务透过端口 143 联机而 IMAPs 服务透过端口 993 联机。	993
Encryption	所谓的 SSL 是利用大数值编码的技术将数据编码后再传至远程，全球信息网在建置之后，必须向一个有公信力的单位登入，并取得一个 Private Key，而将另一个 Public Key 放在网络上；数据在因特网传输时都是经过编码的数据，即使有人在中间要撷取这些经过编码的数据，看到的都是一些毫不具意义的乱码，这种编码的另一种理论基础是，凡是经过 Public Key 编码过的数据，都必须利用 Private Key 才能解的开。	SSL

表格 4-2 IMAP（s）设定

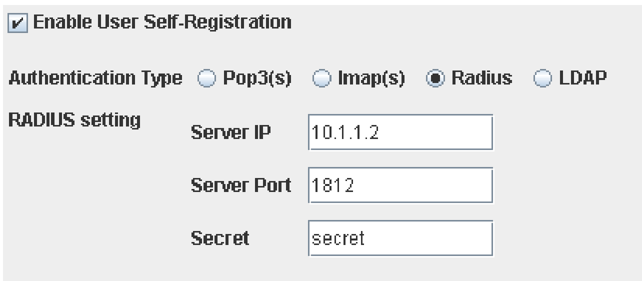
4.2.3 Radius 设定

步驟 1 设定 Radius 验证

如果贵公司已经有安装 Radius 服务器，所有的员工数据都储存在 Radius 服务器中，您可以选择 Radius 验证类别。当用户要自行注册实时通讯账号时，InstantScan 会连络 Radius 服务器提供通行验证。

勾选 **Enable User Self-Registration**（启用验证）。选择 Radius 为验证类型。输入服务器 IP 和服务器端口。输入与 Radius 服务器沟通之Secret 码。然后上传配置文件。

IM Manager > Auth > Radius



字段	说明	范例
Server IP	Radius 服务器 IP 地址。	10.1.1.2
Server Port	Radisu 服务器数据进出的端口。	1812

Secret	Secret 是 Radus 服务器与客户端验证的加密密钥。也就是通讯的各方彼此间共享一把加密密钥，并且利用该密钥的信息来检验彼此的身份。	secret

表格 4-3 Radius 设定

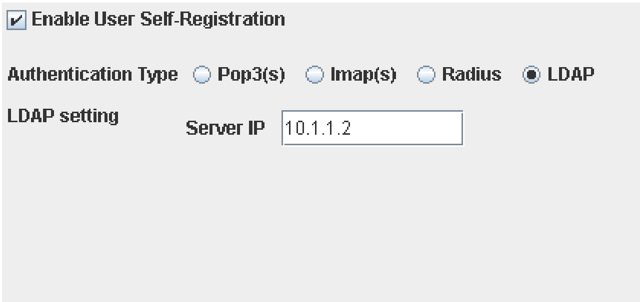
4.2.4 LDAP 设定

步驟 1 设定 LDAP 验证

如果贵公司已经有安装 LDAP 服务器，所有的员工数据都储存在 LDAP 服务器中，您可以选择 LDAP 使用者验证类别。当用户要自行注册实时通讯账号，InstantScan 会连络 LDAP 服务器提供使用者验证，用户只要输入账号与密码，InstantScan 会将此组账号密码传送给 LDAP 服务器验证，一旦通过验证，即可注册实时通讯账号。

勾选 Enable User Self-Registration（**启用验证**）。选择 LDAP 为验证类型。输入服务器 IP，然后上传配置文件。LDAP 相关设定，请参考以下章节。

IM Manager > Auth > LDAP



字段	说明	范例
服务器 IP	LDAP 服务器 IP 地址	10.1.1.11

表格 4-4 LDAP 设定

第3部

InstantScan 管理系统概述

第5章
InstantScan 管理系统介绍

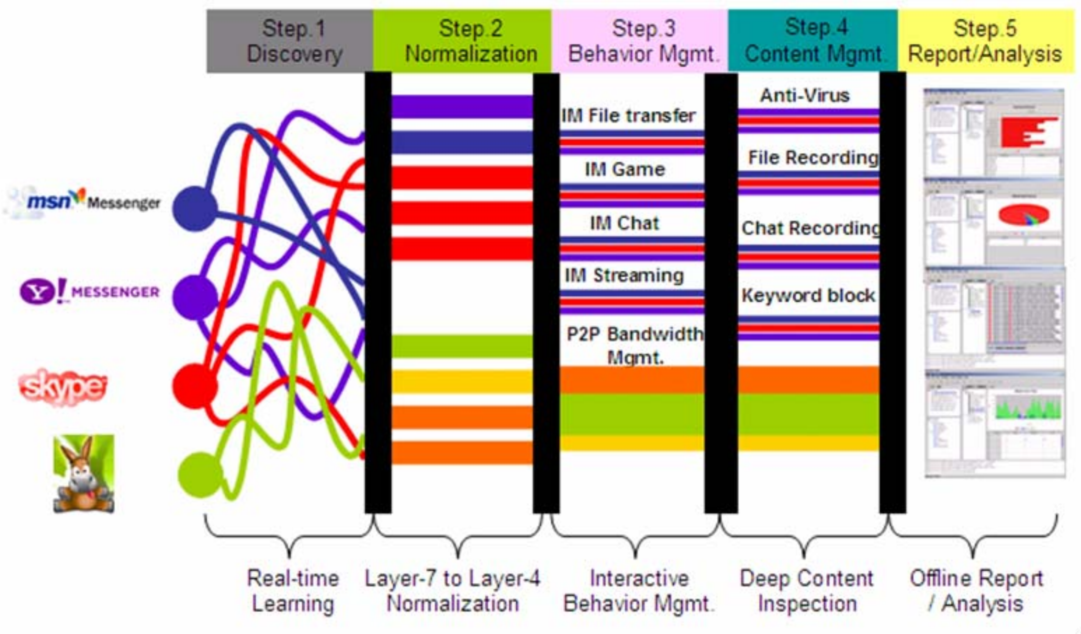
本章节介绍如 InstantScan 的设计原则与设定步骤。

5.1 InstantScan 技术应用

InstantScan 管理系统为一网页应用接口，允许多个管理者同时管理一台或多台 InstantScan装置。您可藉由任何计算机透过网页浏览器来存取 InstantScan 管理服务器。

内容管理五步骤：生产力/安全性最大化、威胁/总持有成本最小化

现今许多因特网用户已经安装了实时通讯（IM）与点对点传输（P2P）应用软件。这些软件会自动随机跳端口，或把自己伪装在 HTTP 的地道里，以规避管理者的检查。为了让管理者克服这个问题，「内容管理五步骤」可用来最大化生产力/安全性，并最小化威胁性与总持有成本。

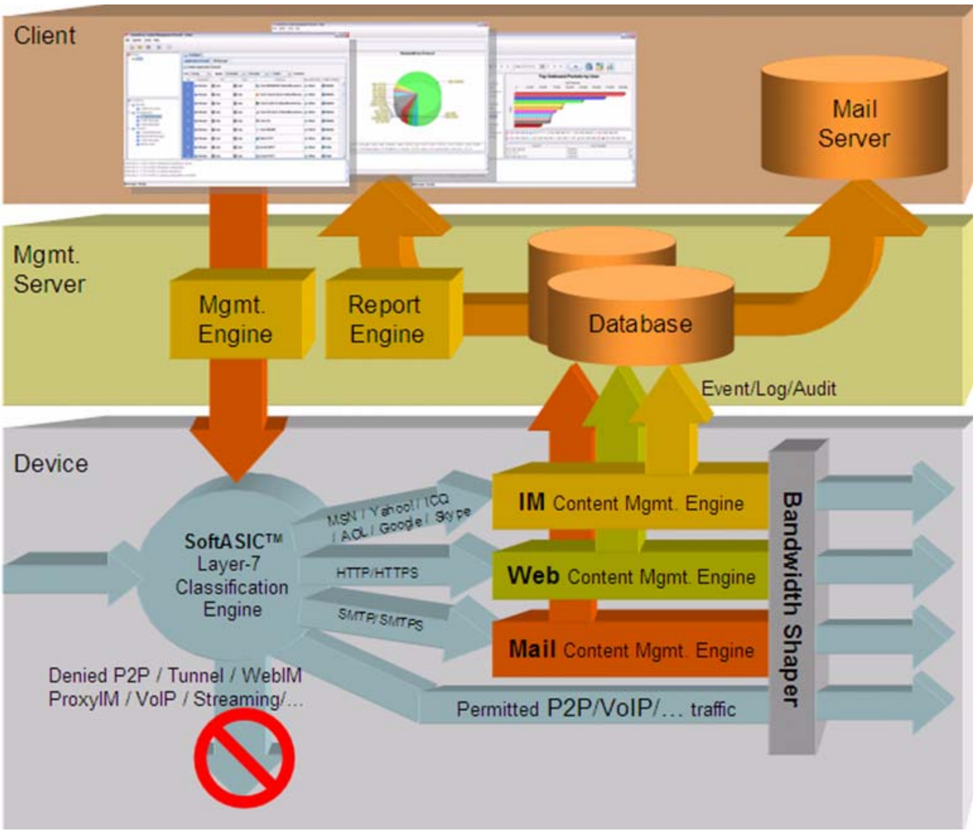


1. 即插即用实时流量侦测/学习：为了帮助管理者解决上述问题，InstantScan 提供了即插即用流量侦测来当作第一步。只需要把网络线接起来，InstantScan 就回现场把网络流量展现在你面前。您可以看到有多少 MSN 是用 HTTP 地道来伪装的，也可以看到有多少 IM 正在聊天。聊天的过程会被自动记录，以方便管理者汇入到设定中。
2. 将第七层流量打回第四层：在流量侦测过后，若是列管的流量，您可以使用第七层防火墙来档掉某些应用。在此图中，InstantScan 会把在第七层乱窜的流量过滤，让其乖乖地以第四层流量方式运行，帮助您原有的第四层防火墙得以用埠号作最基本的控制。非但如此，InstantScan 可说明您阻挡非标准的 IM 联机。例如 MSN 会自动侦测防火墙设定，若 MSN 无法从标准的1860埠号连出去登入，则会开始用 HTTP 代理服务器联机出去。更有甚者，任何人都可以手动设定他要连到哪一台 HTTP/SOCKS4/SOCKS5 代理服务器（包括贵公司里的 HTTP 代理服务器）。最惨的是，员工还可以使用浏览器连到各种不同提供 MSN 服务的网页，继续跟外面的人聊天。这些 InstantScan 都可以帮助您解决。

3. 交互式行为管理：设定个人化的政策。既然 InstantScan 可以认得应用程序的各种细部行为，网管人员可以针对每个使用者给予不同的行为权限。用户的信息可以整合企业现有的用户数据库，例如 LDAP、Active Directory、POP3(S)、IMAP(S)、RADIUS。
4. 深度内容检测：设定进阶的内容过滤功能。在此图中，InstantScan 可侦测/阻挡「压缩文件里的病毒」或「散布在 MSN 窗口里的 URL 或传档蠕虫」。若要做到极端的安全性，所有的对话都可以被侧录，来预防内部信息泄漏。若使用者违反了政策，说了些不该说的话，InstantScan 能够直接在「IM窗口内」警告用户公司的 IM 使用政策
5. 详细报表分析：最后，报表分析可以帮网管人员找出问题。数十种的图形报表，包括每天/每周/每月/每季/每年的带宽报表、IM 使用行为、以公司部门显示聊天侧录、违反政策情况。报表可以客制化、搜寻，且得以用 PDF/HTML/Excel 的格式，在设定的时间周期内以附加文件寄出。

三层式体系结构：效能、可用性、功能最大化

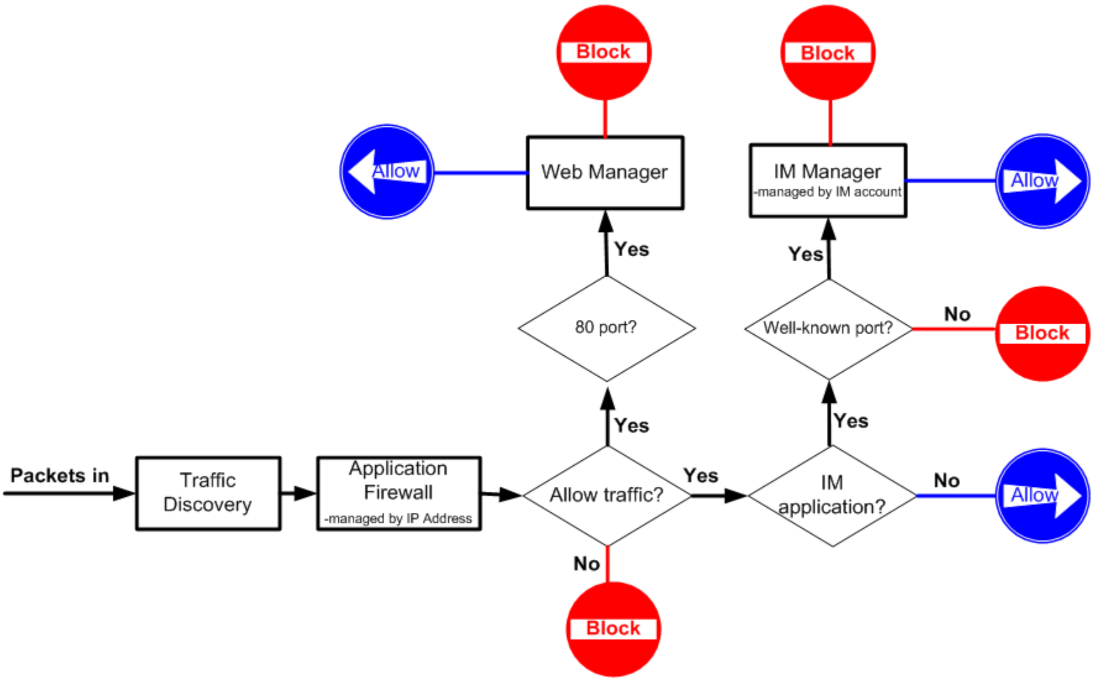
第七层网络设备通常要做「非常多的计算功夫」和「较好的分散架构」，以最大化效能、可用性，与功能性。InstantScan 采用了业界最先进的三层式体系结构来增加效能，让各层各司其职，完成每一个目的。



1. **第七层设备：**第七层设备应该要专注的是「快速地」与「准确地」执行内容检测。如此，第七层设备装在网络进出口在线，才不会影响到网络的效能。
2. **管理服务器：**管理服务器要负责的是中央集中控管第七层设备，并接收来自于不同第七层设备的事件，整理于数据库中更进一步制作报表分析。在管理服务器上制作报表，不会影响第七层设备的效能。
3. **管理客户端：**管理客户端可用任何具备JAVA功能的浏览器连到管理服务器。只要他连得到管理服务器，他就可以连得到任何架设于管理服务器之下的第七层设备。

5.2 内容管理流程

InstantScan 内容管理器可控管时下盛行的实时通讯软件 （IM）、点对点 （P2P） 传输软件、文件传输软件、与远程控管软件、VoIP 软件与网页内容管理等等。您可以藉由这些内容管理项目来做最适当的网络管理，保障公司的网络安全、杜绝一切藉由因特网的便利而机密外泄的管道，更可加强员工的产能。不但可以不用全面封锁实时通讯与点对点传输软件的使用，更可控管这些软件，借助实时通讯、点对点传输软件的时效性与便利性而达到真正公司业务往来省时又省钱的目的。在接下来的章节中，我们将针对内容管理的细项逐一介绍。



图表 5-1 内容管理器之管理流程

如图表 5-1 所示，InstantScan 将进来的流量导给流量监控监看。而当您启用应用层防火墙时，所有应用软件不管是透过 TCP 通讯协议或是代理服务器（例如 HTTP/SOCKS）联机，企图欺骗管理人员，其流经 InstantScan 的封包在经过利基网络第七层辨识引擎辨认后，再依使用者对发送该封包的 IP（来源端）与其送往的对象（目的端 IP）所定义的政策规则决定是否让其通行，只要进来的封包符合设定的条件，就套用该政策规则。

当您启用实时通讯管理员时，MSN/Yahoo/AIM/ICQ 等实时通讯软件将会被规范透过正规的端口联机出去。也就是说 MSN 必须透过端口 1863、Yahoo 5050、AIM/ICQ 5190。如果实时通讯软件透过非正规端口联机，其联机就会被 InstantScan 拦阻。例如，在应用层防火墙允许 MSN 联机，且您亦开启实时通讯管理员并允许 MSN 联机的条件下，MSN_A 透过端口 1863，可以正常联机；而 MSN_B 企图透过端口 80 联机，就会被正规化的政策拦阻。

当网页管理员也启用时，所有透过端口 80 传送的封包都会导给网页管理员监看。管理人员可以依制定的政策做网页内容过滤、URL 侧录、网页扫毒等网页内容管理。

5.3 InstantScan 网页接口设计原则

InstantScan 管理系统包含下列五个窗口：

1. 工具栏：可设定 InstantScan 参数的工具，包含快速功能键。
2. **InstantScan 专案树形图**：包含已选择的项目与受此项目控管的所有装置。
3. **功能树形图**：所有 InstantScan 的功能树形图。包含监看、管理与报表系统等大项。
4. **内容窗口**：各项功能参数的设定窗口。接下来的章节将依序引导您设定 InstantScan。
5. **状态栏**：显示所有系统操作信息。您也可以点击图示 将此状态栏隐藏起来。

5.4 InstantScan 图示说明

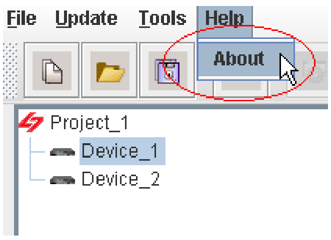
图示		功能
工具栏		新增专案
		开启专案
		显示/隐藏 状态栏
		上传配置文件
内容窗口		物件群组
		单一物件
		除了此选定对象群组外，全部套用该通讯协议的防火墙规则。
		除了此选定对象 （范围/子网/主机） 外，全部套用该通讯协议的防火墙规则。
		日期选项，可依日期期间指定显示选定的事件记录或报表。
		进阶搜寻功能。可依设定的条件搜寻事件记录。
		重新整理事件的时间设定。
		报表导出设定

表格 5-1 InstantScan 图示说明

5.5 工具栏说明

标签	项目	说明
File	Device/Group Manager	建立新装置或群组
	New Project	建立新项目
	Open Project	开启已存在的项目
	Close Project	关闭使用中的项目
	Delete Project	删除选取的项目
	Exit	离开用户网页设定接口
Update	Upload Configuration	上传配置文件到装置上
	Register	进入产品注册网页在线注册您所购买的装置。*您要更新特征码、应用程序行为、病毒/url 数据库或升级韧体前一定要先完成注册手续。
	Update IM engine	从更新中心更新特 IM 引擎
	Update pattern	从更新中心更新应用程序行为
	Update AV database	从更新中心更新病毒数据库
	Update URL database	从更新中心更新 URL 数据库
	License	如果您有购买 Web 模块，您必须在此填写您的授权码，并经过验证后，才可使用。
	Option	更新中心设定
	Support list	InstantScan 所支持的应用程序列表
Tools	Account Manager	依使用层级，设定使用者账号与权限
	Change Password	更改登入密码
	Language Setting	设定语言模块，可选择英文、繁体中文与简体中文三种语言。
	SNMP Control	远程监控设备的系统状态以及网络
	Config Backup	备份现行的配置文件到本地端磁盘
	Config Restore	还原已储存的配置文件到装置上
Help	About	显示 InstantScan 版本讯息

5.6 管理服务器版本

步驟 1 查阅管理服务器版本	Help > About
InstantScan 韧体必须搭配相符的管理服务器版本。请点选 About 查看管理服务器版本。	

步驟 2 显示管理服务器的版本

如右图所示，您可以看到管理服务器的版本与出版的日期。

第6章
阶层式管理与稽核

本章介绍 InstantScan 阶层式管理与稽核的设计与应用。

6.1 需求

面对层出不穷的资安事件，企业为解决资安问题不能单由技术面着手，应藉由建立完整管理系统以有效解决资安问题。根据政府资通会报规定：政府部会中 A、B 级单位需在民国 97 年以前通过 BS7799 认证。由此可见，BS7799 内容的适用性与重要性。此外，由于 BS7799 巨细弥遗的说明企业控管信息安全所应采取的步骤及应制订哪些应变措施。由此可见，BS 7799 是一套完整的计划，能有效建构信息安全防护机制。IT 专业人员可将这套信息安全标准规则当作蓝图，依其导引制定企业的安全政策与程序。InstantScan 内容管理器，为符合 BS7799 的规范，帮助企业执行 BS7799 计划，特地设计阶层式管理与稽核系统。

6.2 目的

内容管理因牵涉到个人隐私与公司机密，在处理上需要特别小心谨慎。InstantScan 阶层式管理与稽核，利用权限控管资安内容，将风险降到最低与资安防护效果最大化，将管理与稽核人员分开，各司其职且相互合作。

6.3 方法

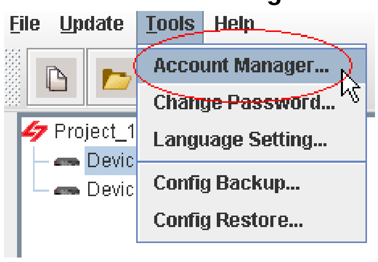
InstantScan目前规划三种权限群组，分别为：

1. **Admin**：管理人员，拥有最高权限，可制定管理政策与浏览侧录讯息。
2. **MIS**：网管人员，可制定管理政策但无法浏览侧录讯息。
3. **Audit**：稽核人员，可浏览侧录讯息，但无法制定管理政策。

6.4 步骤

在您第一次登入 InstantScan 内容管理器时，您可以在账号管理员编辑可存取管理服务器的账号与密码。借由设定的权限阶层式控管 InstantScan，让贵公司确保员工个人隐私与公司机密，更能符合公司稽核的需求。

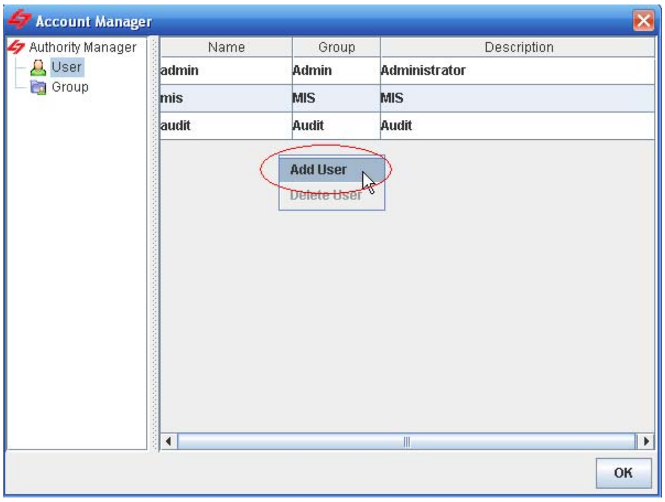
6.4.1 新增使用者账号

步驟 1 管理账号设定 选择 **Account Manager**（账号管理员）选项。	**Tool > Account Manager** 

步驟 2 新增使用者账号

InstantScan 可同时多人联机控管，您可在 Account Manager（账号管理员）建立可存取管理服务器的账号，包含使用者与其所归属的群组。

Tool > Account Manager > User > Add User



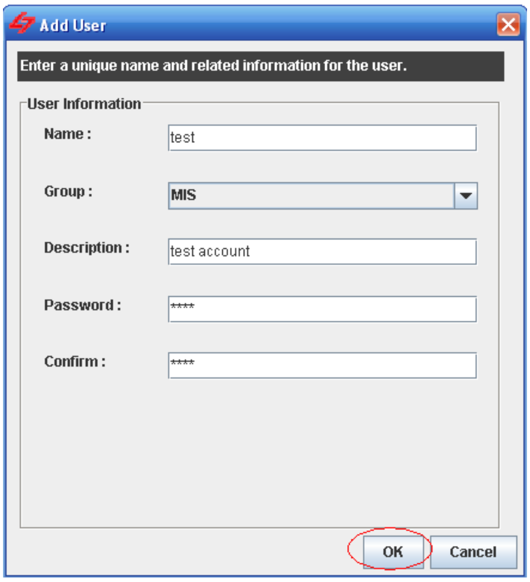
字段	说明	范例
Name（名称）	可存取管理服务器的使用者账号名称。	test
Group（群组）	可存取管理服务器的使用者群组，可分成三种授权群组： 1. admin（管理人员）：可设定 InstantScan、浏览报表与查看侧录记录等所有权限。 2. mis（网管人员）：只可设定 InstantScan，但无法浏览报表与查看侧录记录。 3. audit（稽核人员）：只可查看侧录记录，但无法设定 InstantScan。 **注意：群组不可增删修改。**	mis
Description（描述）	针对账号的详细说明。	test account

表格 6-1 账号管理员

步驟 3 编辑账号

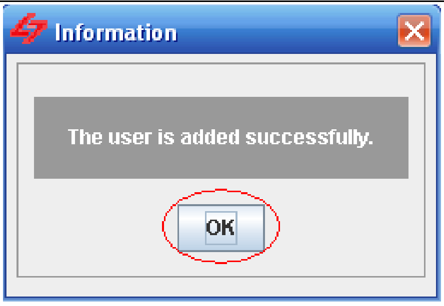
请输入您要新增的账号名称、对此账号的描述、与其密码，并选择所属群组。点击 **OK** 完成设定。

Tool > Account Manager > User > Add User



步骤 4 账号建立成功讯息

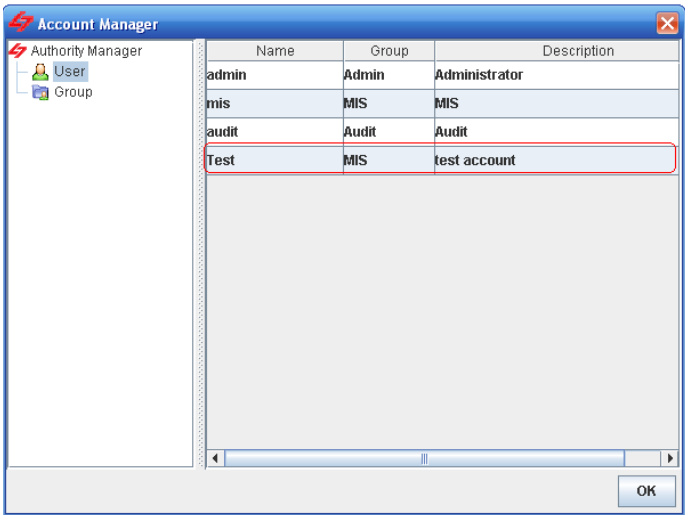
当您建立账号成功，将有如右图的窗口通知您新增成功。



步骤 5 显示已增加的账号

当您成功建立账号，您可以在 **Account Manager**（账号管理员）的窗口上看到这笔数据。

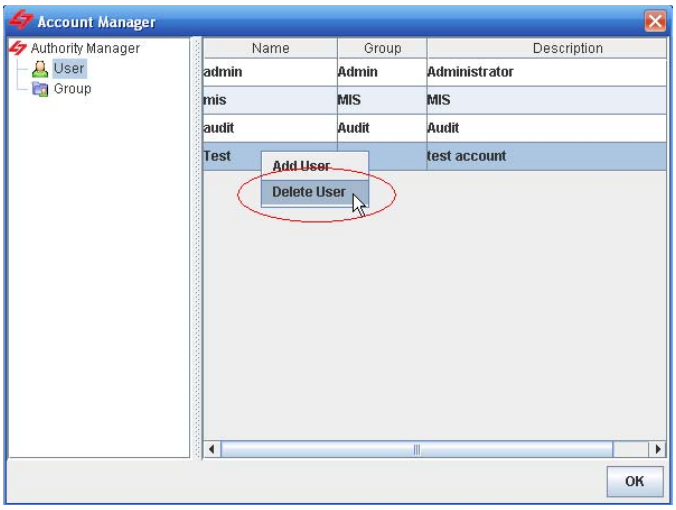
Tool > Account Manager > User



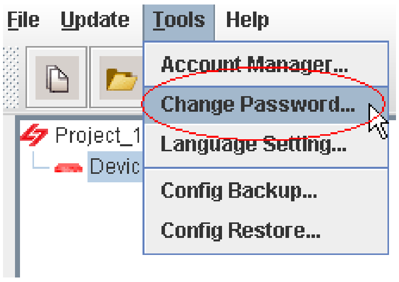
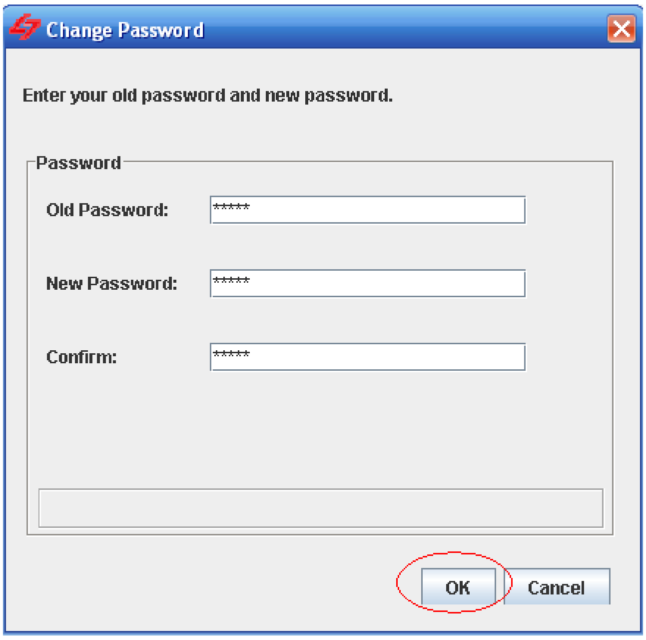
步骤 6 删除账号

欲删除某笔账号，只要点选此笔数据，然后右键单击，选择 **Delete User** （删除使用者）即可。

Tool > Account Manager > User > Delete User



6.4.2 修改用户登入网页接口的密码

<table>
<tr>
<td>步驟 1 点选更改密码
选择 Change Password（更改密码）选项。</td>
<td>Tool > Change Password

</td>
</tr>
<tr>
<td>步驟 2 输入新的密码
输入 Old Password（旧的密码）与 New Password（新的密码），然后在 Confirm（确认）字段内再次输入新的密码。点击 OK 完成设定。</td>
<td>Tool > Change Password

</td>
</tr>
</table>

第4部

网络监看

第7章
网络监看

本章节介绍网络监看的应用。

7.1 监看公司网络

InstantScan Traffic Discovery （流量监控）功能，让所有流经 InstantScan 装置的流量丨览无遗地呈现在管理者的眼前。管理者可以藉由检视网络流量来决定针对特定流量管理的方式，用以避免带宽遭到员工滥用。MSN/Yahoo/ICQ/AIM 等实时通讯软件，当其企图透过非正规的端口联机，系统将会以红字标示，将此联机显示在 Traffic Discovery 上。透过 Traffic Discovery，网管人员可实时看到整过网络的使用状况，进而做最适当的带宽控管。

步驟 1　监看网络状态

在Traffic Discovery上点两下，您可一目了然目前网络的联机状况。以红字标示的联机为经由非正规端口之联机。请注意，Traffic Discovery 为一树状结构，第一层为通讯协议、第二层为正在使用此通讯协议的 IP 地址，第三层为该 IP 地址使用此通讯协议的联机状况。

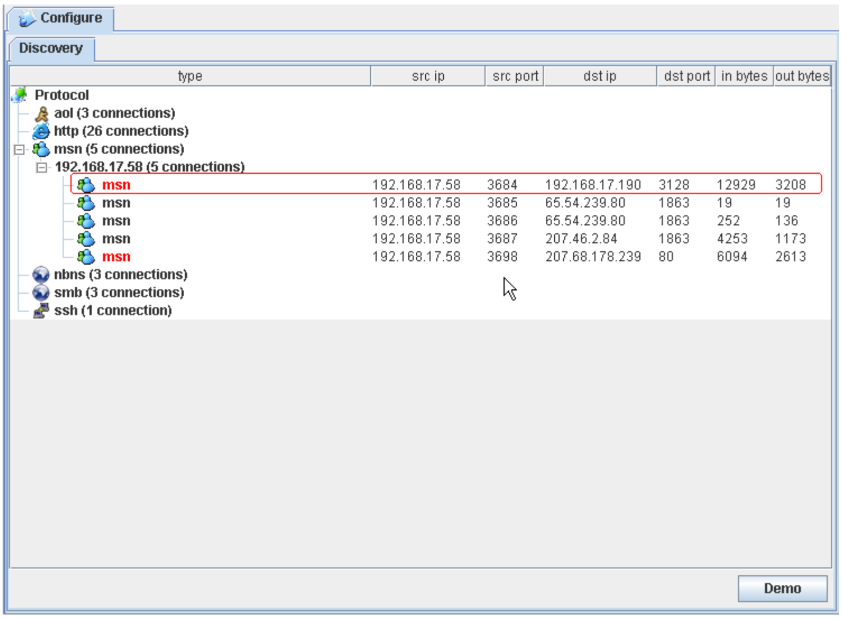
注意，所谓正规端口为：

MSN：1863

Yahoo：5050

AIM/ICQ：5190

Function > Monitor > Traffic Discovery > Dicovery



字段	说明	范例
Type	通讯协议的类别。当某通讯协议以红字标记时，代表此联机透过非正规端口联机。	msn
Src IP	流经InstantScan的封包之来源端 IP 地址。	192.168.17.58
Src port	流经InstantScan的封包之来源端端口。	3684
Dest IP	流经InstantScan的封包之目的端 IP 地址。	192.168.17.190
Dest port	流经InstantScan的封包之目的端端口。	3128
In bites	选定联机的对内流量大小。	12929
out bites	选定联机的对外流量大小。	3028

表格 7-1 流量监控字段解释

第5部

对象管理员

第8章
对象管理员 – IP 与 Schedule

本章介绍 IP 与排程的设定与使用方式。

8.1 需求

1. ABC 公司希望管理公司内部的所有 IP 的网络使用权限。但是，CEO 与 CTO 有完整的权限存取因特网的资源。
2. ABC 公司的上班时间是星期一早上 8:30 – 12:00，下午 13:00 – 17:30。中午 12:00 – 13:00 为午休时间。依公司政策，某些实时通讯或点对点传输软件在上班时间不准使用。
3. 性质相同的对象最好能够将其群组一起以方便政策规则的设定。

8.2 方法

1. 点选 InstantScan 对象管理员之地址，设定 CEO 的 IP 地址为 192.168.168.2，CTO 的 IP 地址为 192.168.168.10，并将此两个都是管理阶层的地址对象群组在一起。
2. 在对象管理员之排程设定上班时间，并将不连续的上班时间群组成一个排程。

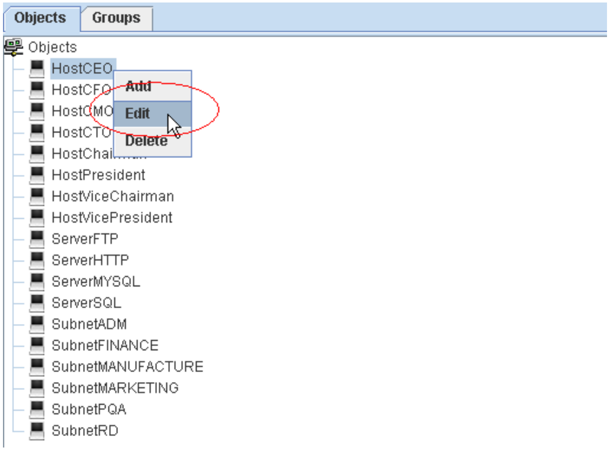
8.3 步骤

8.3.1 地址设定

步骤 1 新增对象地址

在 **HostCEO** 上右键单击，然后选择 **Edit**。为了您制定规则的便利性，InstantScan已默认一些常用的地址对象供您选择使用，您可以直接修改默认的 IP 地址，或将默认对象删除，然后自行新增对象。

Function > Management > Object Manager > Address > Objects



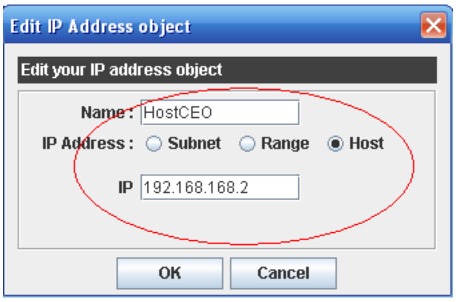
步骤 2 编辑 HostCEO

将 HostCEO 默认的 IP 地址改成 192.168.168.2。您亦可根据贵公司的网络架构，变更此对象的名称与 IP 地址。

IP 地址可以是 **1）Subnet**（子网）；**2）Range**（范围）；或 **3）Host**（主机）。

对象HostCEO设定亦同。

Function > Management > Object Manager > Address > Objects



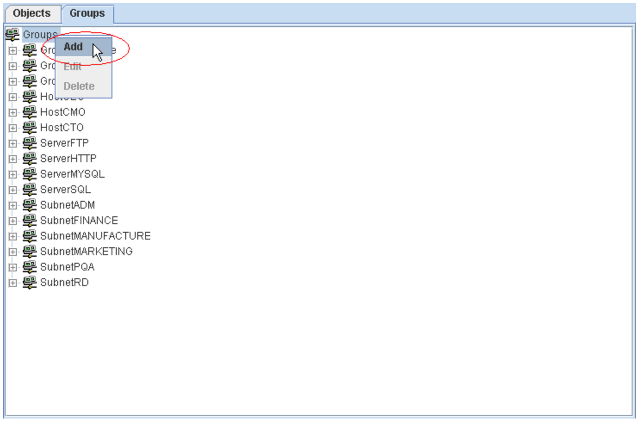
IP Address		说明	范围 / 格式	范例
Subnet	IP	子网 IP 地址	IPv4 格式	192.168.168.0
	Mask（0-32）	子网掩码	子网掩码格式	24
Range	Start IP	此对象范围的起始 IP 地址。	IPv4 格式	192.168.168.1
	End IP	此对象范围的结束 IP 地址。	IPv4 格式	192.168.168.10
Host	IP	单一主机 IP 地址。	IPv4 格式	192.168.168.2

表格 8-1 定义地址对象

步骤 3 新增物件群组

在屏幕上右键单击，然后点选 **Add**。

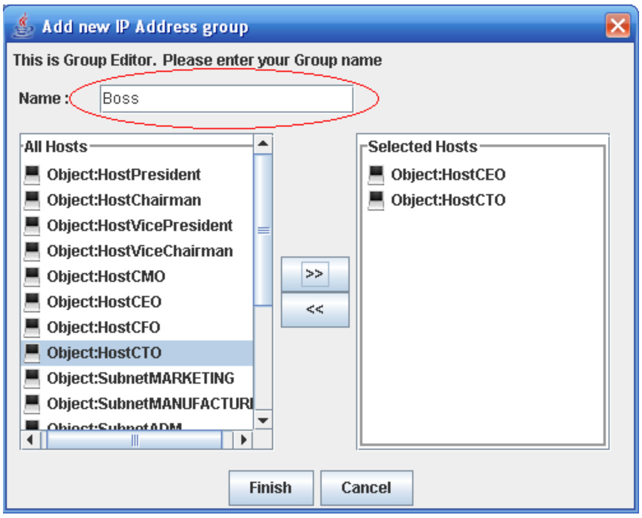
Function > Management > Object Manager > Address > Groups



步骤 4 编辑群组

在名称字段内输入 **Boss**，在 All Hosts 字段内选择 **Object:HostCEO** 与 **Object:HostCTO**，然后点击 **>>** （右向箭头），将此两个地址对象加到 **Selected Hosts** 字段内。欲移除群组中某个地址对象，请在 Selected Hosts 字段内选择要移除的对象，然后点击 **<<**（左向箭头）即可。

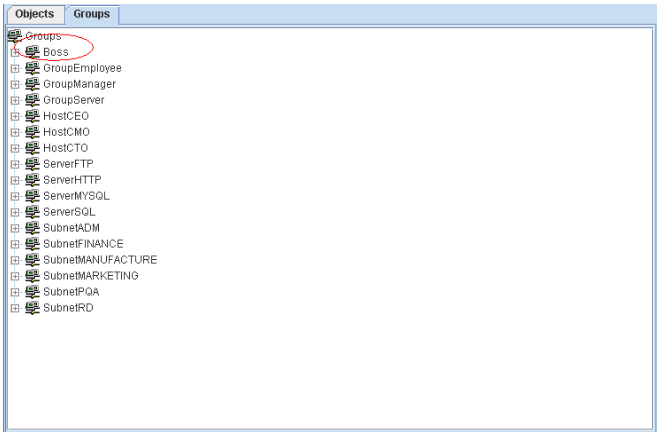
Function > Management > Object Manager > Address > Groups



步骤 5 显示已建立的群组

当您点击 **Finish** 按钮后，已建立的群组将显示在屏幕上。如右图所示。

Function > Management > Object Manager > Address > Groups



步驟 6 上传配置文件到装置中

点选 **Upload Configuration** 选项，或者点击 图标，将现行的配置文件上传到装置上。

⚠ 如果某个对象已经被某个群组或某条政策规则所使用，在删除此对象前，您必须先删除包含此对象的地址群组或是政策规则，否则您无法删除此对象。

8.3.2 排程设定

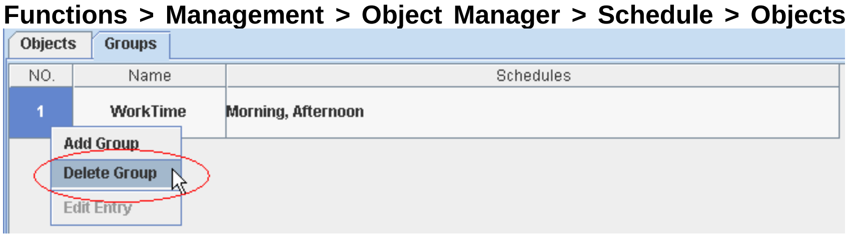
步驟 1 删除预设排程

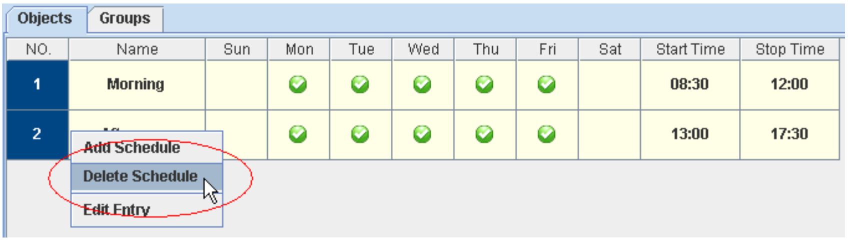
InstantScan已提供您两条预设的排程，如果预设的排程不符您的需求，您可以修改此排程，或者将其直接删除。

在接下来的范例中，我们将删除默认的排程规则，然后透过新增排程介绍您排程的设定。
请注意，在删除排程前请先确认排程群组或其他政策规则是否已经含有此排程了。

右边的例子为排程对象已经被排程群组所使用了，所以您必须先删除排程群组，然后才可删除排程对象。

Functions > Management > Object Manager > Schedule > Objects

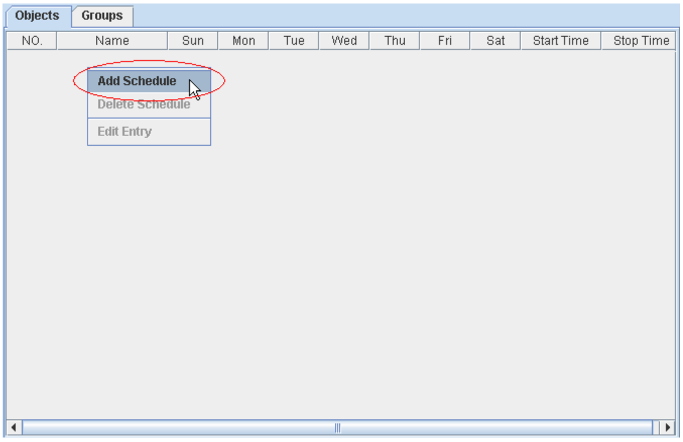


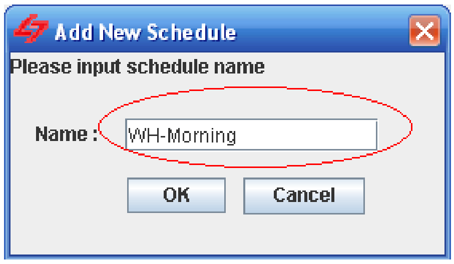
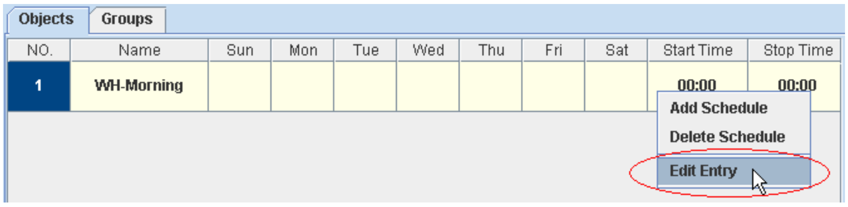
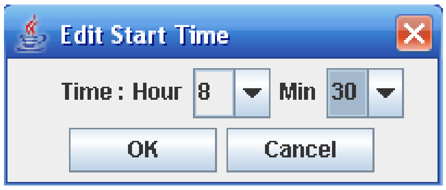
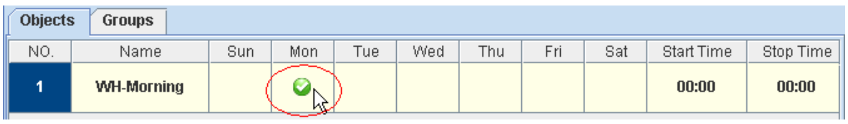
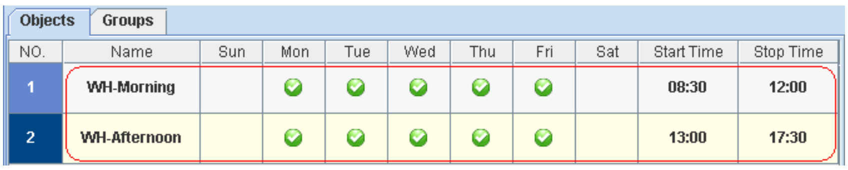


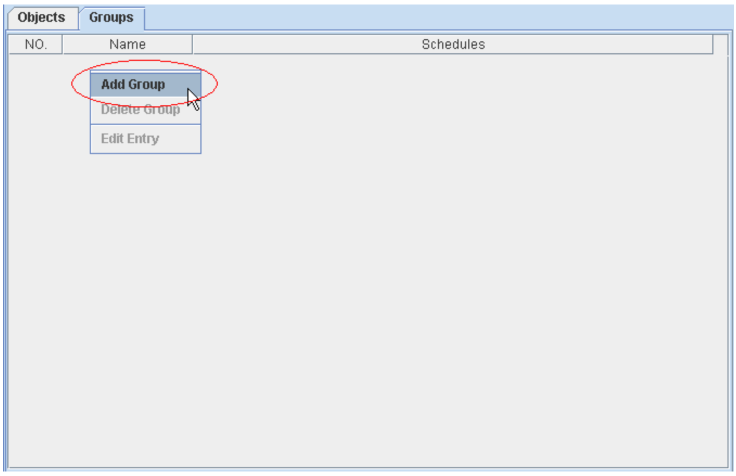
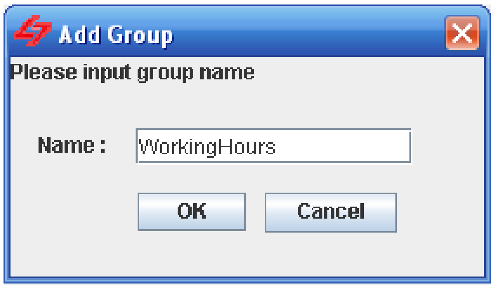
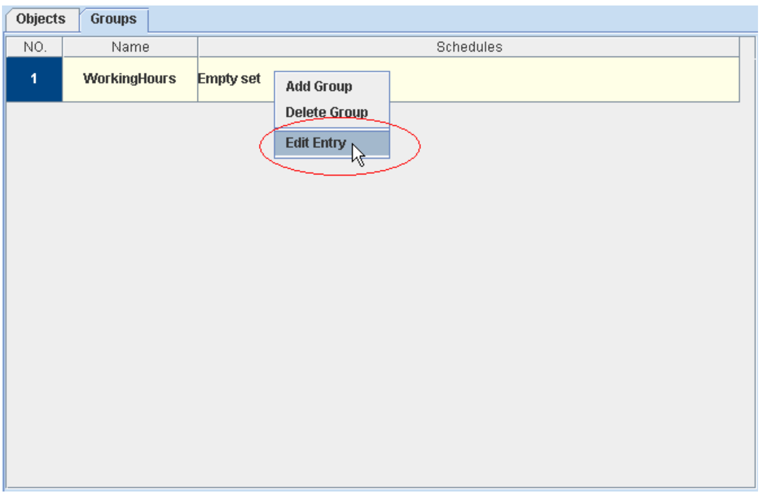
步驟 2 在排程对象屏幕上右键单击

在屏幕上右键单击，然后点击 **Add Schedule** 选项。

Functions > Management > Object Manager > Schedule > Objects



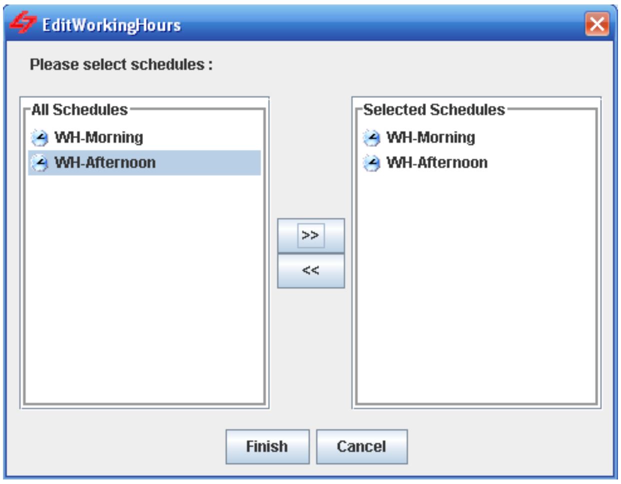
步驟 3 新增排程 输入排程名称。点击 **OK** 关闭窗口。	**Functions > Management > Object Manager > Schedule > Objects** 
步驟 4 编辑时间 在 WH-Morning 规则的 **Start Time** 字段上右键单击，然后点选 **Edit Entry** 选项。	**Functions > Management > Object Manager > Schedule > Objects** 
步驟 5 拉选起始时间 拉选 **Start Time** 的时与分，然后点击 **OK** 关闭窗口。 Stop Time 的设定相同，请参照起始时间的设定。	**Functions > Management > Object Manager > Schedule > Objects** 
步驟 6 日期管理 ABC公司的上班时间为星期一到星期五，所以您必须将鼠标移动到 **Mon** 字段上点一下，即有一图示  显示在表格内。接下来设定 Tue ~ Fri。 其他排程的设定皆相同。	**Functions > Management > Object Manager > Schedule > Objects** 
步驟 7 浏览排程设定结果 现在，我们已经设定好了两条排程。您可以开始将这两条排程群组一起了。	**Functions > Management > Object Manager > Schedule > Objects** 

<table>
<tr>
<td>步驟 8 新增群组
因为ABC公司的上班时间为 8:30~12:00 与 13:00~17:30，所以您必须将此两个不连续的时间群组在丨起，以方便管理规则的建立。在屏幕上右键单击，然后选择 Add Group 选项。</td>
<td>Functions > Management > Object Manager > Schedule > Groups

</td>
</tr>
<tr>
<td>步驟 9 输入组名
输入组名，然后点击 OK 关闭窗口。</td>
<td>Functions > Management > Object Manager > Schedule > Groups

</td>
</tr>
<tr>
<td>步驟 10 编辑群组
在 WorkingHours 规则的 Schedule 字段上右键单击，然后选择 Edit Entry 选项。</td>
<td>Functions > Management > Object Manager > Schedule > Groups

</td>
</tr>
</table>

步驟 11 编辑群组

在 All Schedules 字段内选择您要加入此群组的排程，然后点击 **>>** （右向箭头），将选定的排程加入 Selected Schedules 字段内。如果您要移除某个在此群组中的排程，请在 Selected Schedules 字段中点选该排程，然后点击 **<<** （左向箭头）即可移除。点击 **Finish** 结束设定。

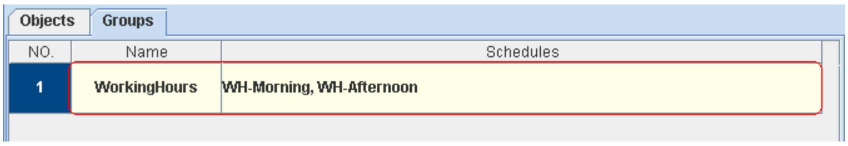
Functions > Management > Object Manager > Schedule > Groups



步驟 12 检视已设定的排程群组

在您完成上列设定后，画面将回到排程群组的首页，您可以在此检视您的设定。

Functions > Management > Object Manager > Schedule > Groups



步驟 13 上传配置文件到装置上

点选 **Upload Configuration** 选项，或者点击图标  上传配置文件到装置中。

⚠ 如果某个对象群组已经被某条政策规则所使用，在删除此群组前，您必须先删除包含此群组的政策规则，否则您无法删除此群组。

第6部

流量管理员、应用层防火墙

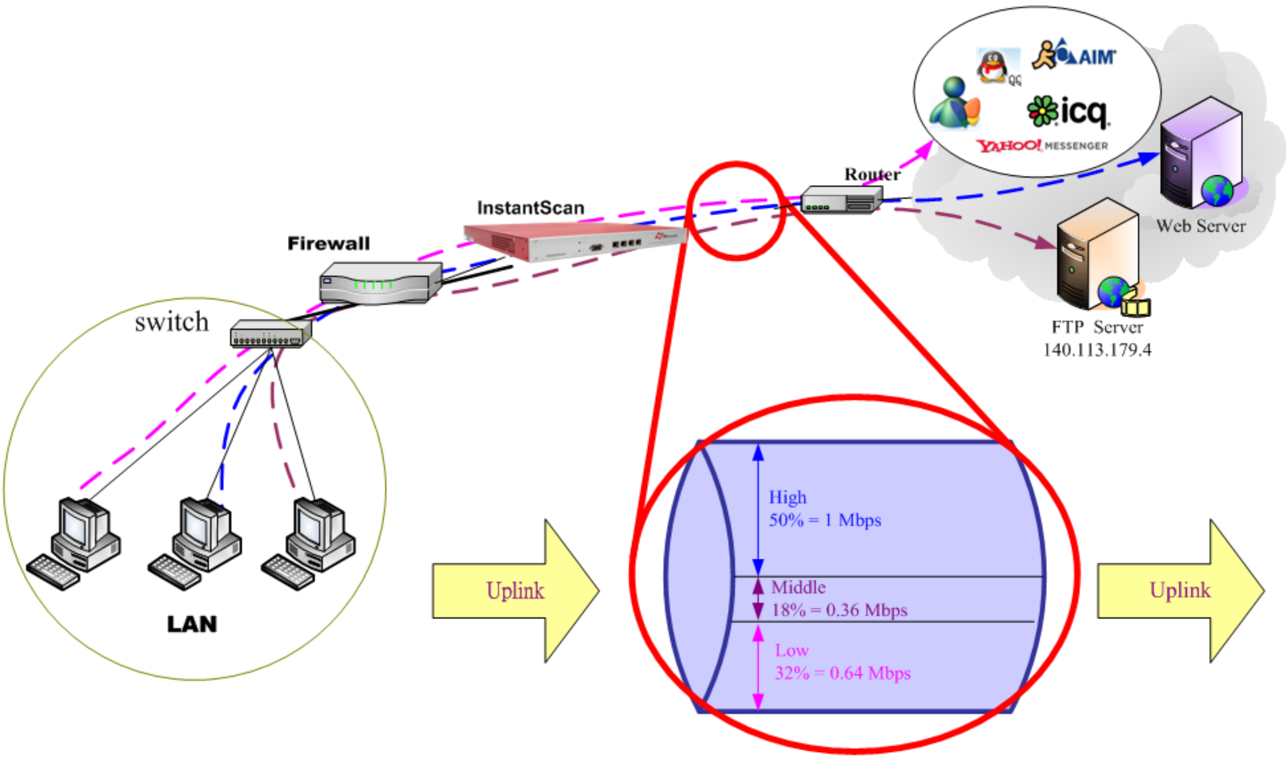
第9章
流量管理员

本章介绍 Traffic Manager 与其使用方式。

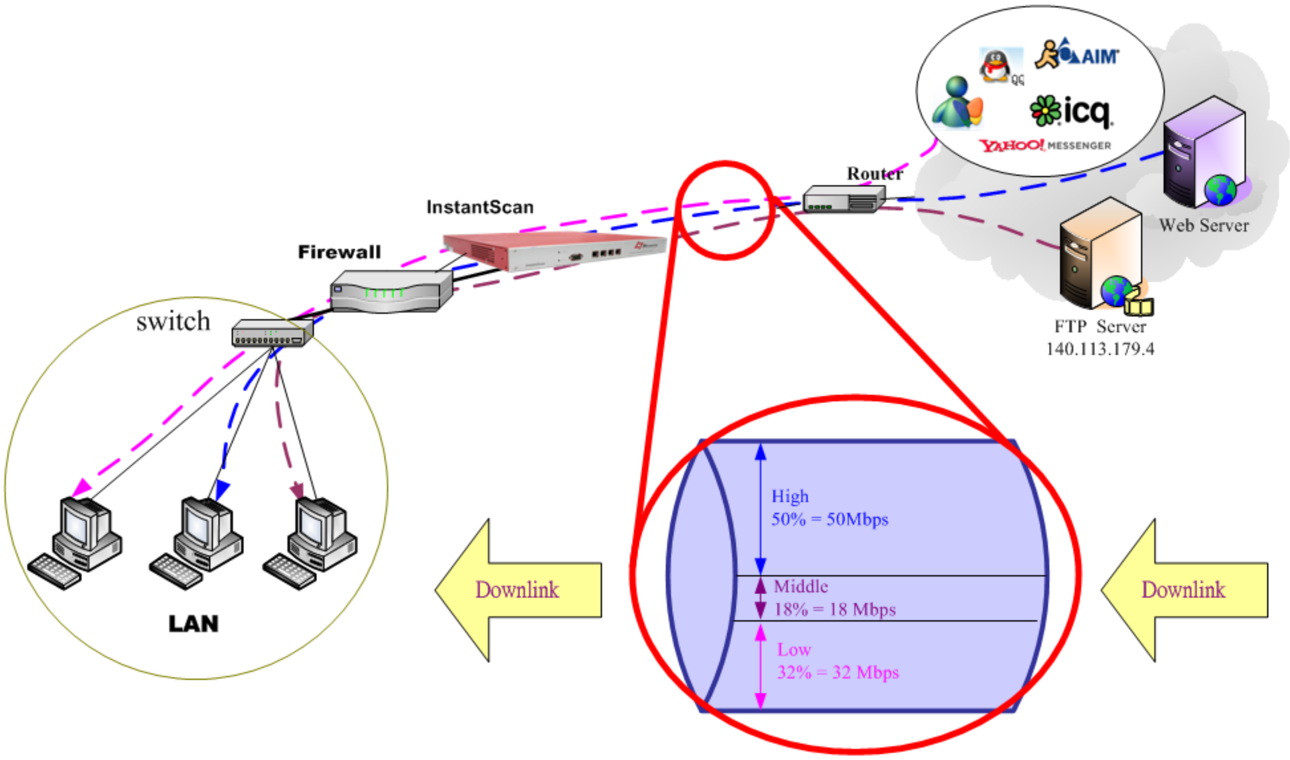
由于因特网的盛行，员工上网随时随地都可以上传或下载数据/档案，滥用带宽的结果常导致重要讯息/档案无法实时传送/接收，造成公司莫大的损失。有鉴于滥用带宽的事件频仍，InstantScan 流量管理员设计用来管理时下盛行的应用软件之带宽。借由鼠标拖拉的动作即可有效的控管带宽，省时省力又大大提升网络带宽的应用效率。

9.1 需求

为了让网络带宽能够做最适当的安排，管理者希望将 FTP 服务分类成中 （**Middle**） 类别，并且限制中类别只可占对外或对内之总带宽的 18%。详见下列图表。



图表 9-1 对外带宽管理



图表 9-2 对内带宽管理

9.2 方法

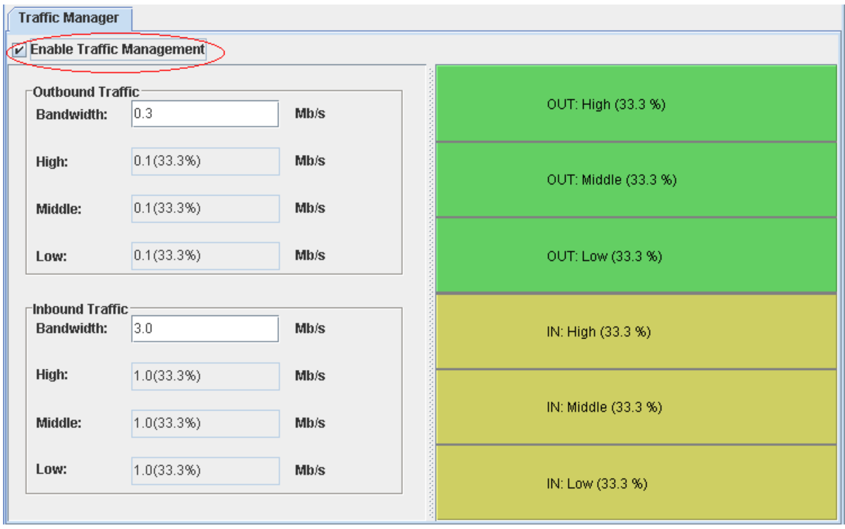
InstantScan 分别将对外与对内流量区分成三个类别，如下表所示。对外流量的总带宽为 2Mbps，而对内流量的总带宽为 100 Mbps。

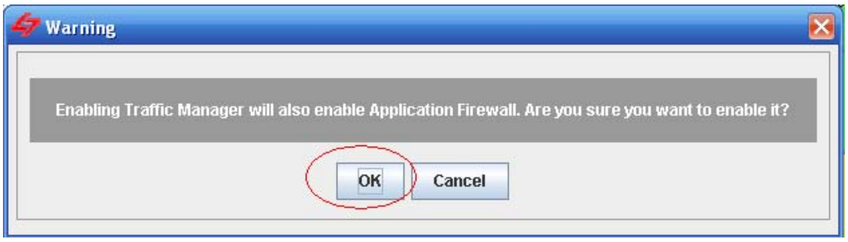
带宽流向	总带宽	类别	带宽分配
对外流量	2 Mbps	高 （High）	50% = 1 Mbps
		中 （Middle）	18% = 0.36 Mbps
		低 （Low）	32% = 0.64 Mbps
对内流量	100 Mbps	高 （High）	50% = 50 Mbps
		中 （Middle）	18% = 18 Mbps
		低 （Low）	32% = 32 Mbps

依上表所示，如果某个应用软件被归类为低类别，其最大对外带宽限制为 0.64 Mbps，其对内带宽限制为 32 Mbps。例如，MSN/Yahoo/ICQ/AOL/GoogleTalk 等实时通讯软件皆被归类为低类别，那么 MSN + Yahoo + ICQ + AOL + GoogleTlak + Webim = 32 % 总对外或对内带宽，也就是说其对外带宽为 2 * 32% = 0.64 Mbps，而对内带宽为 100 * 32% = 32 Mbps。

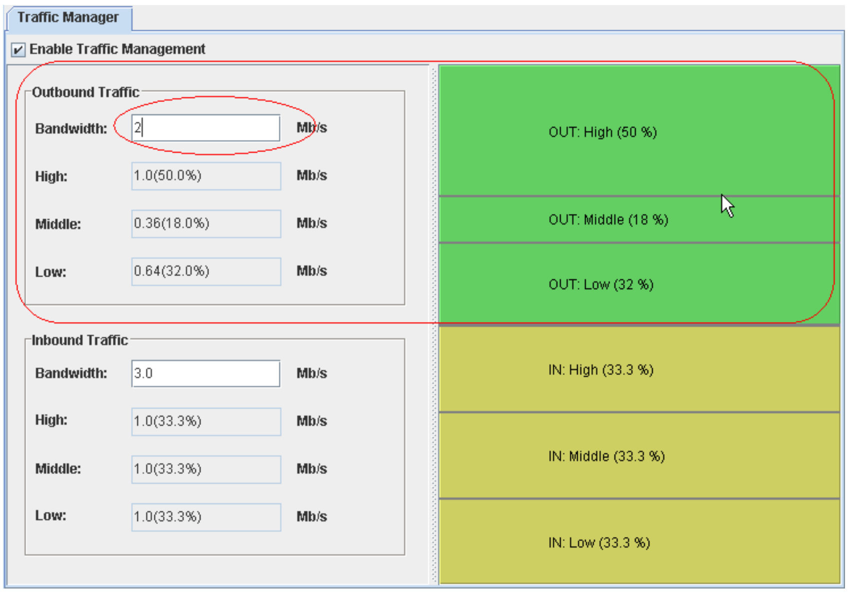
9.3 步骤

<table>
<tr>
<td>步骤 14 启用流量管理
勾选 Enable Traffic Management。</td>
<td>Functions > Management > Traffic Manager > Traffic Manager



</td>
</tr>
<tr>
<td>步骤 15 警告讯息
当您启用流量管理员时，系统同时间亦会将应用层防火墙启用。</td>
<td>

</td>
</tr>
<tr>
<td>步骤 16 订定对外流量
在 Outbound Traffic 字段内输入 2 。利用鼠标拖拉右边的带宽控制线，让 High 类别占 50% 总带宽，Middle 类别占 18% 总带宽，而 Low 类别占 32% 总带宽。当您设定好带宽大小后，带宽的分配状况即会显示在左边带宽类别字段上。</td>
<td>Functions > Management > Traffic Manager > Traffic Manager

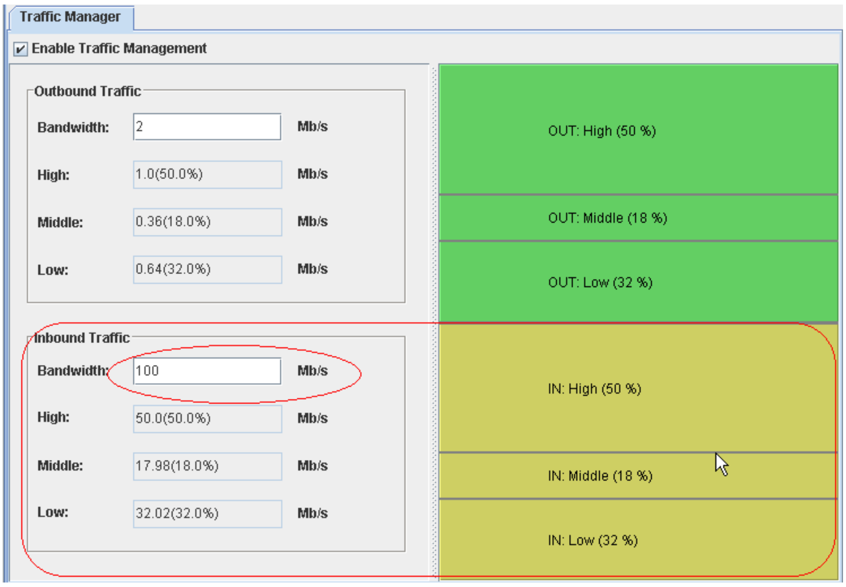


</td>
</tr>
</table>

步驟 17 订定对内流量

同 Outbound Traffic 设定。在 Inbound Traffic 字段内输入**100**。利用鼠标拖拉右边的带宽控制线，让 High 类别占 50% 总带宽，Middle 类别占 18% 总带宽，而 Low 类别占 32% 总带宽。当您设定好带宽大小后，带宽的分配状况即会显示在左边带宽类别字段上。

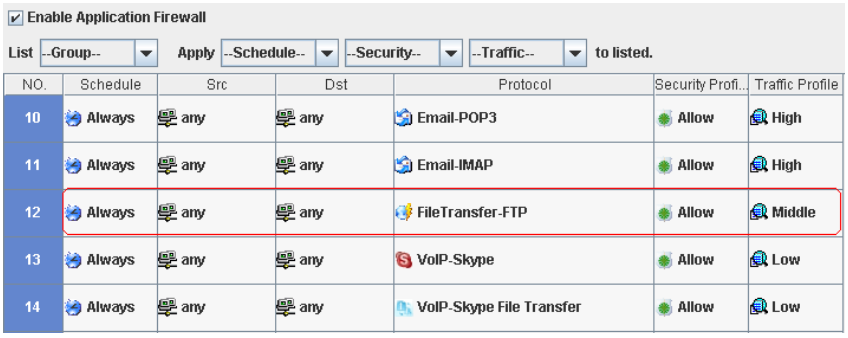
Functions > Management > Traffic Manager > Traffic Manager



步驟 18 启用应用层防火墙

请检查启用应用层防火墙是否已经勾选。如图表 9-1 与图表 9-2 所示，将 FTP 服务的带宽类别设定为 Middle，并允许其流量通行。

Functions > Management > Application Firewall



步驟 19 上传配置文件

点选 Upload Configuration 选项，或点击图标 将现行的配置文件上传到 **InstantScan** 装置上。

第10章
应用层防火墙

本章节介绍应用层防火墙与其设定。

10.1 应用防火墙介绍

根据 2005 年 5 月 Gartner 提出的「Application Delivery and Web Application Firewall Are Ready to Converge」报告中指出，现今所有的网络攻击事件中，约有 75%的攻击事件是瞄准应用层，我们可以发现网络攻击已经不仅是单纯的扫瞄网段或主机，而是以企业必须开启的端口为发动攻击开端，为了确保网络安全，「应用层防火墙（Application Firewall）」是最佳的防御方式。

应用层防火墙只是一个防御环节，最重要的还是相对应的防御政策。所以应用层防火墙必须根据其所需保护的应用程序定义不同的防御政策。以目前应用程序网页化的趋势而言，小至网页邮件、大至整个企业的 ERP 系统，都可以透过浏览器使用，我们可以想见网页服务器攻击的比例将会越来越高，而防护难度也相对提升。InstantScan 的应用层防火墙系将所有通过该装置的应用软件加以辨识控管，让企业阻绝一些不必要的应用，且透过带宽控管，让企业内部的网络可发挥其最大的功效。

10.2 需求

1. CEO 与 CTO 拥有完整的权限可以使用因特网资源。
2. 除了 MSN 以外，上班时间不允许使用其他实时通讯软件。
3. 除了 Skype 以外，上班时间不允许使用其他点对点传输软件。
4. 上班时间，R&D 部门不允许使用 Skype 传档。

10.3 方法

1. 允许所有来自 CEO 与 CTO 的网络流量。
2. 除了 CEO 与 CTO 外，员工在上班时间内只允许使用 MSN，其余实时通讯软件一律拦阻。
3. 除了 CEO 与 CTO 外，员工在上班时间内只允许使用 Skype 传送简讯与档案，其余点对点传输软件与 VoIP 一律拦阻。
4. 上班时间不允许 R&D 部门的员工透过 Skype 传档。

10.4 步骤

1. 启用应用层防火墙、设定上班时间排程、允许所有来自 Boss 群组的网络流量、允许 MSN 并拦阻其余实时通讯软件的使用。
2. 允许 Skype 并拦阻其余点对点传输软件的使用。
3. 上班时间，拦阻 R&D 部门的 Skype 文件传输。

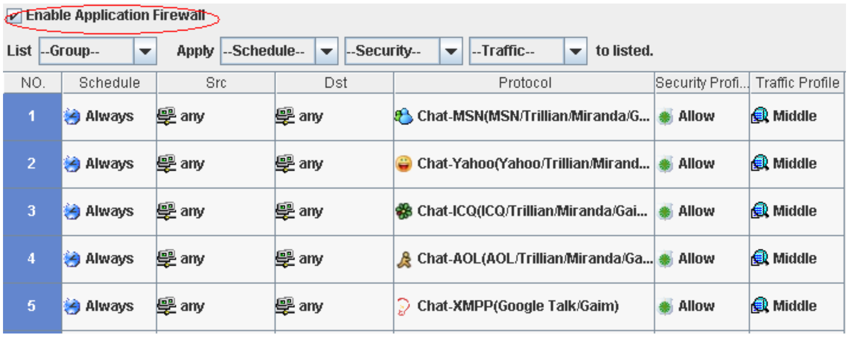
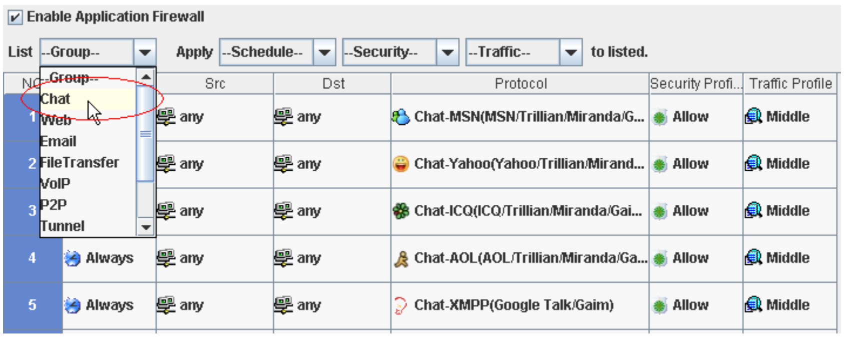
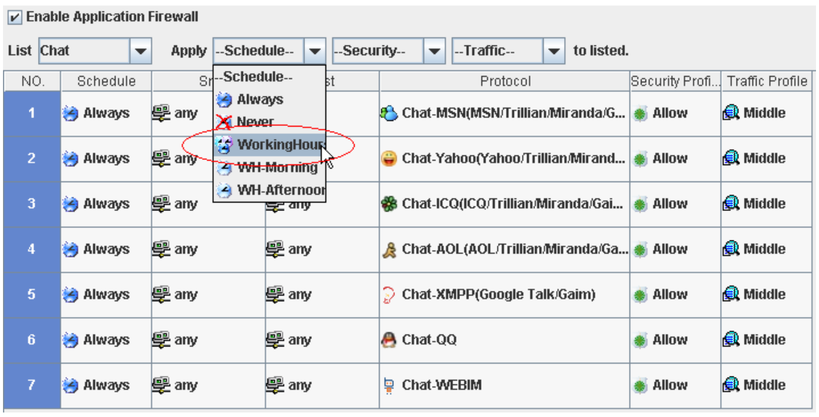
⚠ **注意：**

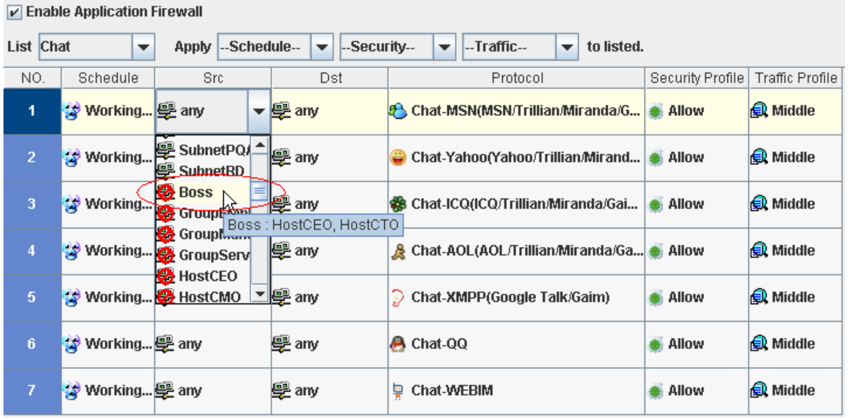
1. 如果您选择让某个应用软件通过 InstantScan，不管其来源端/目的端的 IP 地址为何，所有属于该应用软件的流量皆可通过 InstantScan。

---

2. 如果 InstantScan 摆放在贵公司防火墙外，且透过防火墙转址，因 InstantScan 本身设计上的考虑，您无法透过特定的 IP 控管任何应用软件。且 Traffic Discovery 上所看到的来源端 IP 都是防火墙的 WAN 端 IP，无法显示其真实的 IP。

10.4.1 设定实时通讯软件规则

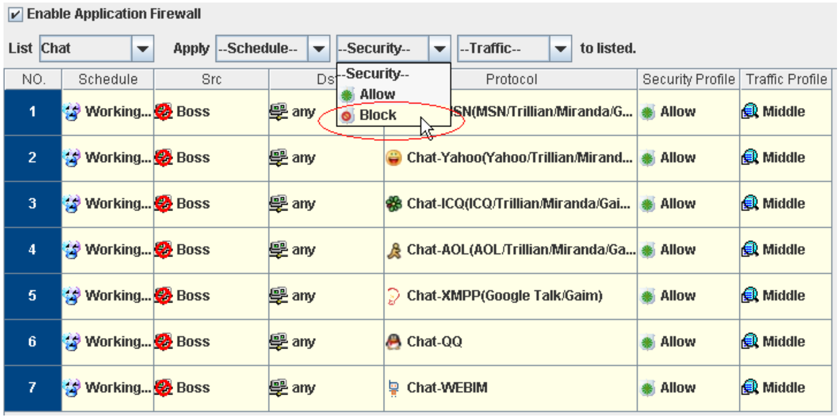
步驟 1 启用应用层防火墙 勾选 **Enable Application Firewall**。	**Function > Management > Application Firewall** 
步驟 2 列举 **Chat** 群组 在搜寻工具栏上选择 **List Chat**，列举所有属于 Chat 群组的规则。	**Function > Management > Application Firewall** 
步驟 3 选择排程 在工具栏上选择Apply **WorkingHours** 排程，将此排程套用在所有 **Chat** 群组中。您亦可以手动选择每条应用程序行为的排程。	**Function > Management > Application Firewall** 
步驟 4 选择来源端 **IP** 因为CEO与CTO有完整的权限存取因特网资源，且在上一章节中我们已建立一群组 **Boss** （**HostCEO, HostCTO**）。选择图示 Boss，意味着除了 **Boss** 这个群组外，所有来源端 IP 使用实时通讯软件都套用选定的应用层防火墙规则。	**Function > Management > Application Firewall**



步驟 5 选择安全行为（Security Profile）

在工具栏的 **Security** 选项上选择套用 **Block** 在所有实时通讯应用软件上，但是请记得之后要将 MSN 的 Security 选择**Allow**。因为依公司规定，上班时间允许使用 MSN。

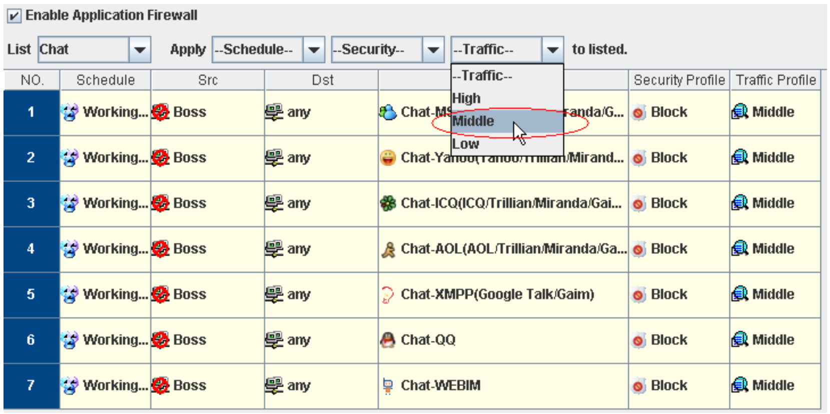
Function > Management > Application Firewall



步驟 6 选择带宽类别（Traffic Profile）

在工具栏的 Traffic 选项上选择套用 Middle 在所有实时通讯应用软件上。使所有实时通讯软件的带宽限制为 Middle 类别。

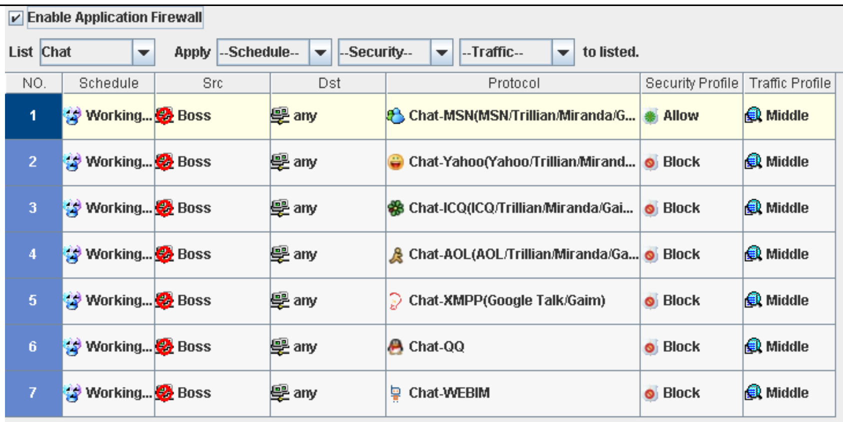
Function > Management > Application Firewall



步驟 7 浏览已设定好的实时通讯政策

浏览已设定好的实时通讯政策规则。

Function > Management > Application Firewall



字段		说明	范围 / 格式	范例
List	Group	依群组搜寻所有应用层防火墙规则，并列举搜寻结果。	所有 InstantScan 定义的群组	Chat
Apply ______ to listed.	Schedule	将选取的排程规则套用在所列举的清单中。	使用者定义	WorkingHours
	Security Profile	将选取的安全行为规则套用在所列举的清单中。	Allow / Block	Block
	Traffic Profile	将选取的带宽类别规则套用在所列举的清单中。	High / Middle / Low	Middle

表格 10-1 应用层防火墙功能列

字段	说明	范围 / 格式	范例
Src	进入 InstantScan 之封包的来源端 IP 地址。请注意，图示 Boss 指的是除了 Boss 这个地址群组外的其余 IP 地址。	Subnet / Range / Host	Boss
Dst	进入 InstantScan 之封包的目的端 IP 地址。请注意，图示 Boss 指的是除了 Boss 这个地址群组外的其余 IP 地址。	Subnet / Range / Host	any
Protocol	通讯协议类别，或是可受 InstantScan 控管的应用程序类别。	所有可控管的通讯协议	Chat-MSN
Security Profile	控管应用程序的使用行为。	Allow / Block	Allow
Traffic Profile	在流量管理员中所定义的带宽类别。	High / Middle / Low	Middle

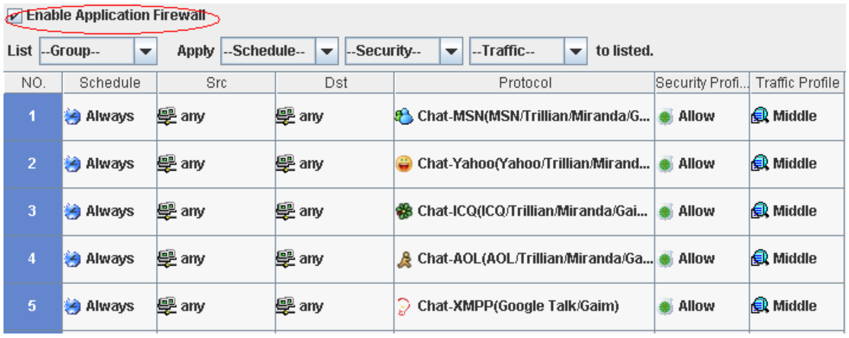
表格 10-2 应用层防火墙字段说明

10.4.2 设定点对点传输软件规则

步驟 1 启用应用层防火墙

勾选 **Enable Application Firewall**。

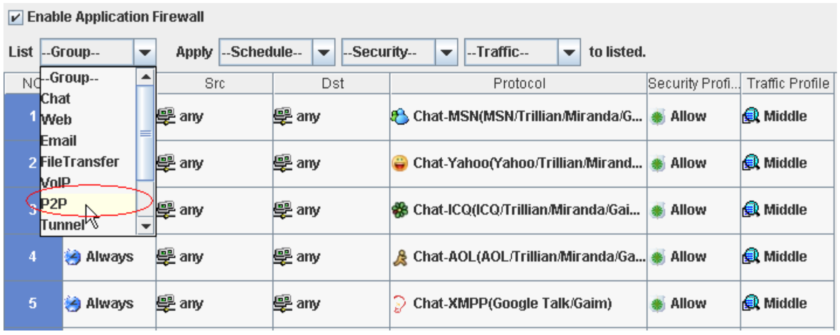
Functions > Management > Application Firewall



步驟 2 列举 **P2P** 群组

在工具栏之 **Group** 上选择 **List P2P** 。所有P2P的列表就会显示在屏幕上。

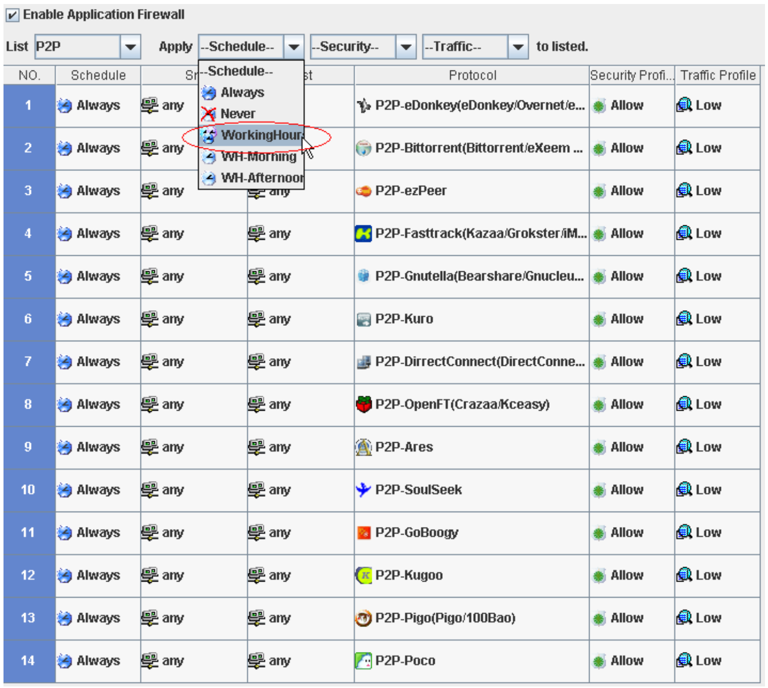
Functions > Management > Application Firewall



步驟 3 选择排程

在工具栏上选择 **WorkingHours** 排程，将此排程套用在所有 **P2P** 群组中。您亦可以手动逐一选择适合选定政策的排程。

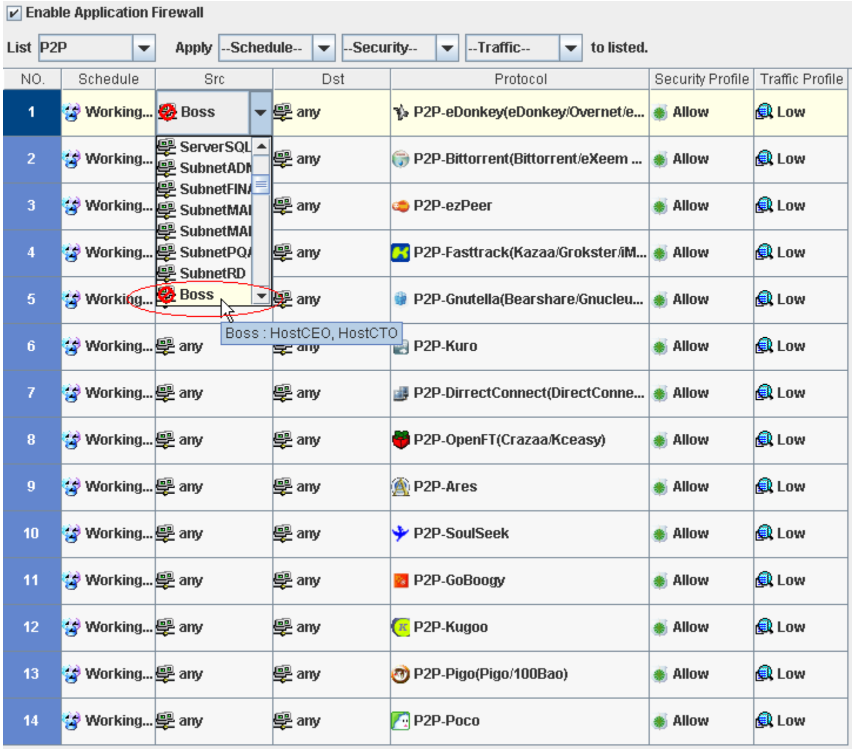
Functions > Management > Application Firewall



步驟 4 选择来源端 IP

因为CEO与CTO有完整的权限存取因特网资源，且在上一章节中我们已建立一群组 **Boss**（**HostCEO, HostCTO**）。选择图示 **Boss**，意味着除了 **Boss** 这个群组外，所有来源端 IP 使用点对点传输软件都套用选定的应用层防火墙规则。

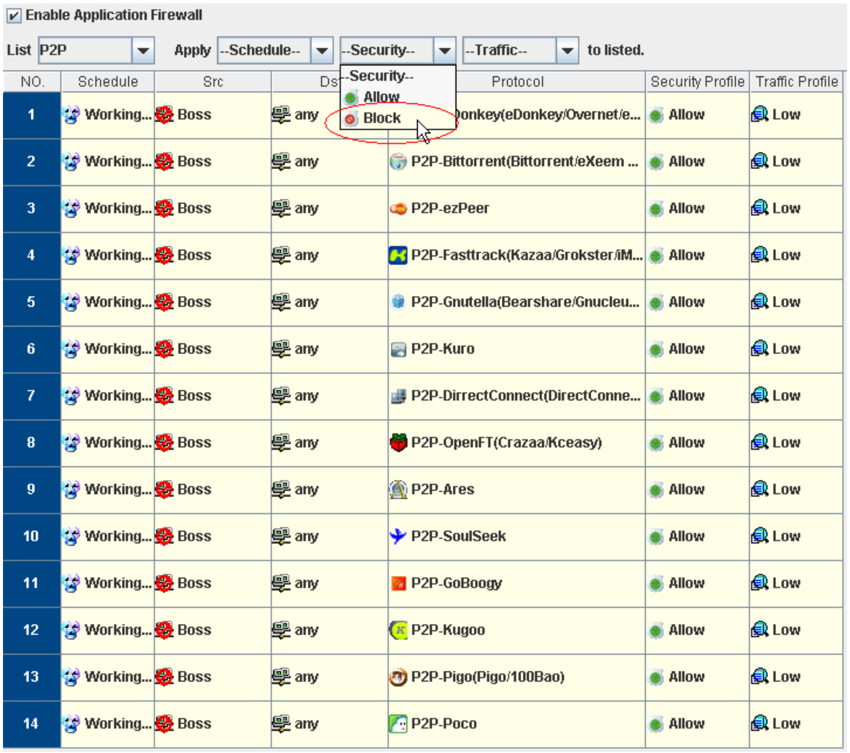
Functions > Management > Application Firewall



步驟 5 选择安全行为

在工具栏的 **Secuirty Profile** 选项上选择套用 **Block** 在所有点对点传输软件。

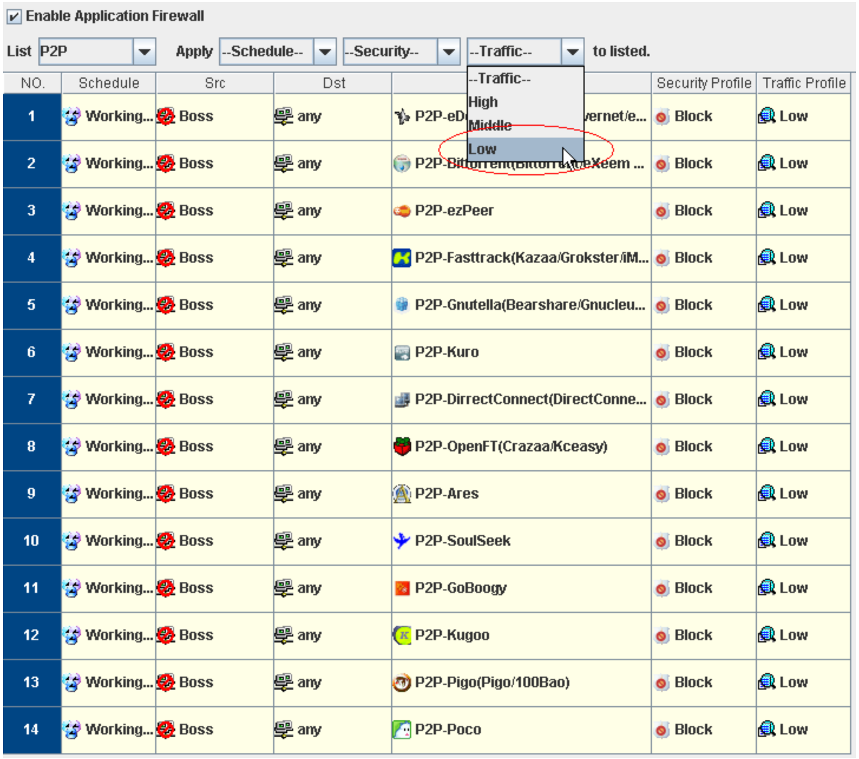
Functions > Management > Application Firewall



步驟 6 选择带宽类别

在工具栏的 Traffic Profile 选项上选择套用 **Low** 类别在所有点对点传输软件上。使所有实时通讯软件的带宽限制为 **Low** 类别。

Functions > Management > Application Firewall

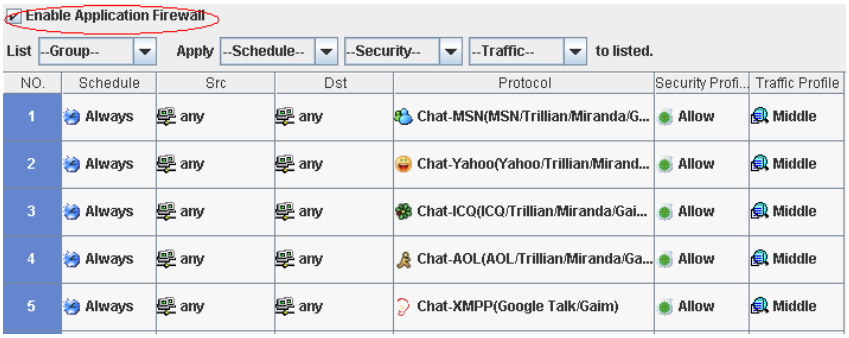


10.4.3 设定 VoIP 规则

步驟 1 启用应用层防火墙

勾选 **Enable Application Firewall**。

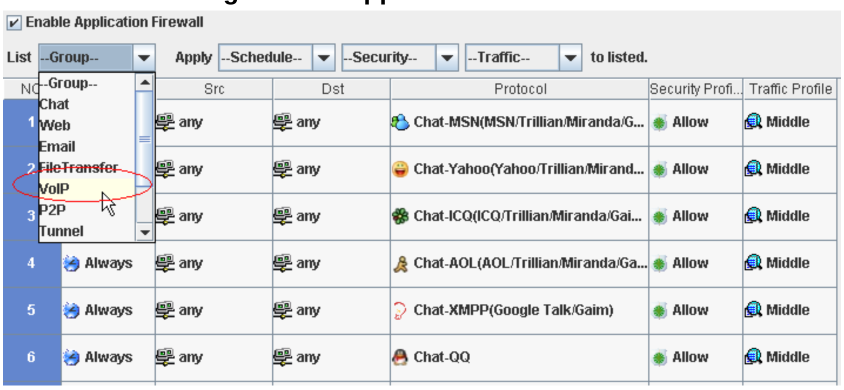
Functions > Management > Application Firewall



步驟 2 列举 VoIP 群组

在工具栏之 **Group** 上选择 **List VoIP**。所有VoIP 的列表就会显示在屏幕上。

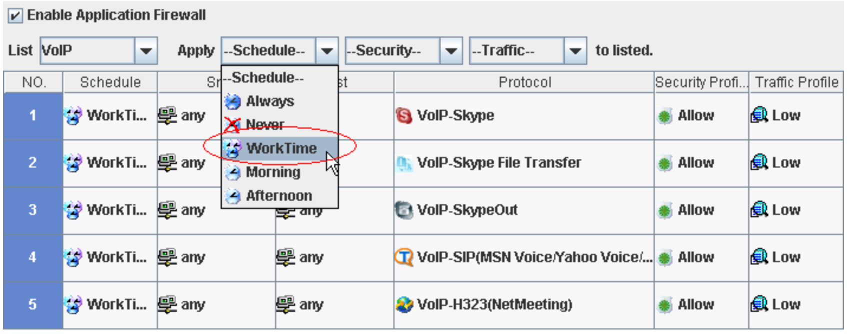
Functions > Management > Application Firewall



步驟 3 选择排程

在工具栏上选择 **WorkingHours** 排程，将此排程套用在所有 **VoIP 群组**中。您亦可以手动选择每条应用程序行为政策的排程。

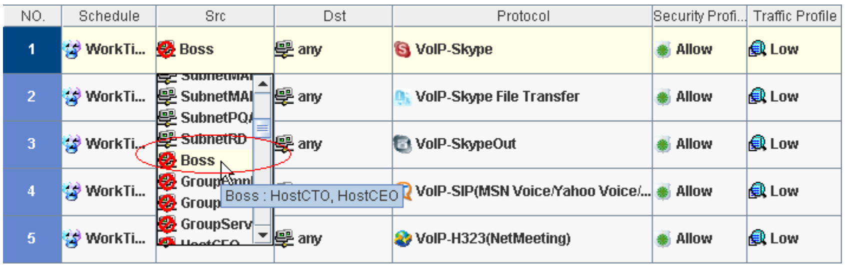
Functions > Management > Application Firewall



步驟 4 选择来源端 IP

因为CEO与CTO有完整的权限存取因特网资源，且在上一章节中我们已建立一群组 **Boss**（**HostCEO, HostCTO**）。选择图示 Boss，意味着除了 **Boss** 这个群组外，所有来源端IP使用点对点传输软件都套用选定的应用层防火墙规则。

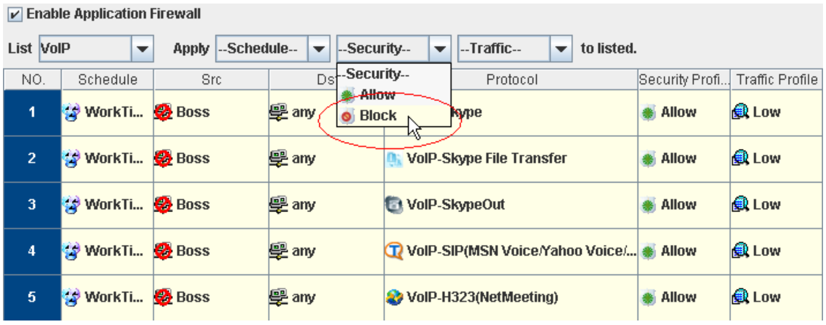
Functions > Management > Application Firewall



步驟 5 选择安全行为

在工具栏的 **Security Profile** 选项上选择套用 **Block** 在所有点对点传输软件上。

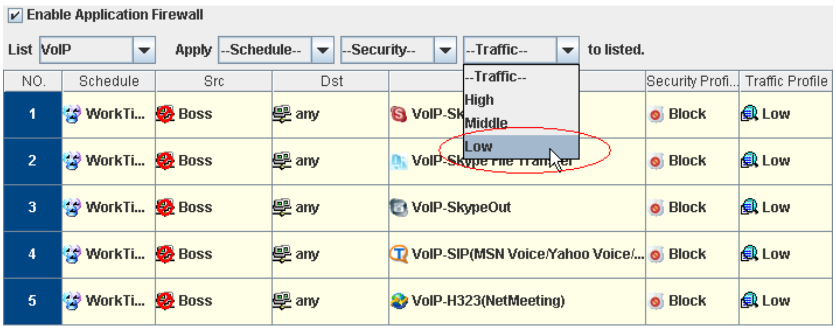
Functions > Management > Application Firewall



步驟 6 选择带宽类别

在工具栏的 **Traffic Profile** 选项上选择套用 **Low** 在所有点对点传输软件上。使所有实时通讯软件的带宽限制为 **Low** 类别。

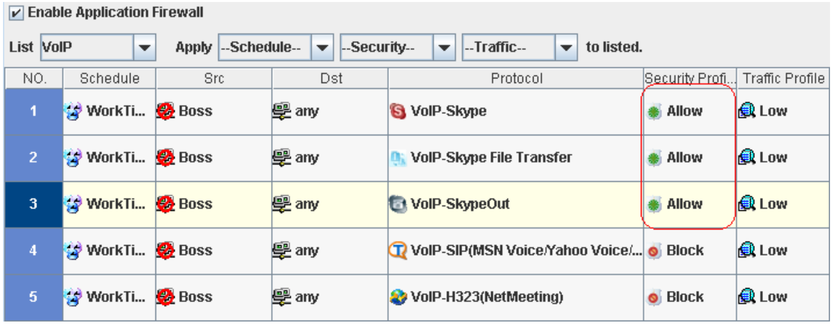
Functions > Management > Application Firewall



步驟 7 调整 Skype 的安全行为

依公司政策允许员工上班使用 Skype，所以您必须手动调整 Skype 的安全行为到 **Allow** 的状态。这样 Skype 的流量才可以通过InstantScan。

Functions > Management > Application Firewall



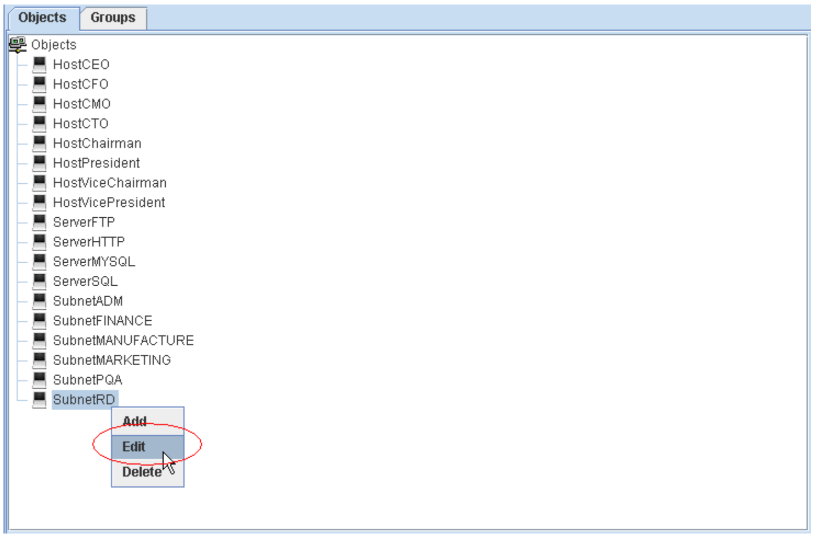
10.4.4 拦阻 VoIP - Skype File Transfer

步驟 1 检查对象管理员

因为R&D部门不可使用 Skype 的文件传输功能，所以包含在 R&D 部门的 IP 地址范围，从 192.168.17.1 ~ 192.168.17.254，属于 192.168.17.0 之网段。请先编辑好对象 SubnetRD，然后才可编辑 Skype的规则。

在 SubnetRD 上右键单击，然后点击 **Edit**。

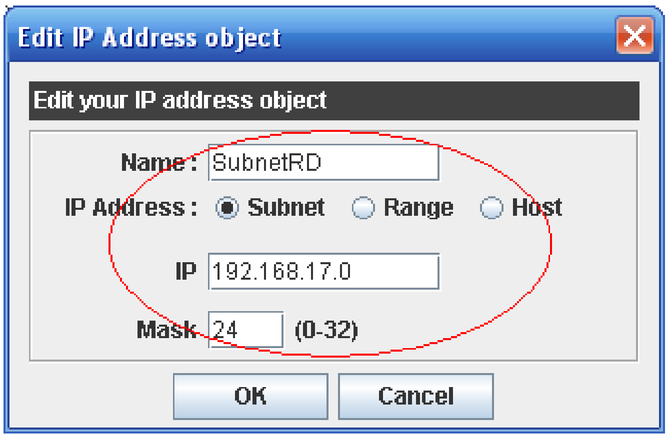
Functions > Management > Object Manager > Address > Objects



步驟 2 设定R&D部门的IP地址

地址对象可以是子网、范围、单一主机。SubnetRD 的地址性质属于子网，所以请编辑 SubnetRD 为 192.168.17.0/24。 点击 **OK** 关闭窗口。

Functions > Management > Object Manager > Address > Objects



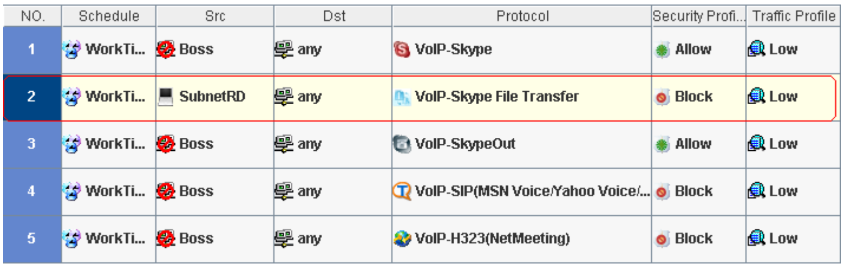
步驟 3 上班时间拦阻 R&D 部门员工使用 Skype文件传输

根据 ABC 公司的政策，所有VoIP应用软件只开放使用 Skype，但是 R&D 部门的员工因为机密性因素，在上班时间不准使用 Skype 文件传输。

上一节我们已设定好 VoIP 的使用规则了，现在要将其加以调整。点选 VoIP-Skype File Transfer，在 Src 字段上选择 SubnetRD 选项，然后在 Security Profile 上选择 **Block**。

当 RD 想透过 Skype 传档时，这个动作就会被 InstantScan 拦阻下来。

Functions > Management > Application Firewall



NO.	Schedule	Src	Dst	Protocol	Security Profi...	Traffic Profile
1	WorkTi...	Boss	any	VoIP-Skype	Allow	Low
2	WorkTi...	SubnetRD	any	VoIP-Skype File Transfer	Block	Low
3	WorkTi...	Boss	any	VoIP-SkypeOut	Allow	Low
4	WorkTi...	Boss	any	VoIP-SIP(MSN Voice/Yahoo Voice/...	Block	Low
5	WorkTi...	Boss	any	VoIP-H323(NetMeeting)	Block	Low

步驟 4 上传配置文件

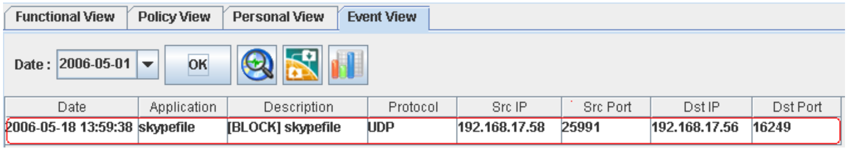
当设定好以上的政策规则后，请记得上传配置文件到InstantScan装置上，否则当您重新连上装置后，现行的配置文件就会被系统清除。

选择 **Upload Configuration** 选项，或者点击图标 上传现行的配置文件。

步驟 5 Skype传文件的事件记录

由右图我们可以看出，RD 部门 IP 192.168.17.58 企图透过 Skype 传档，但被 InstantScan 拦阻下来的事件记录。

Functions > Reports > Application Firewall > Event View



Date	Application	Description	Protocol	Src IP	Src Port	Dst IP	Dst Port
2006-05-18 13:59:38	skypefile	[BLOCK] skypefile	UDP	192.168.17.58	25991	192.168.17.56	16249

设定小技巧：

1. 如果您要选取/取消选取某条规则时，只要利用 ＜Ctrl＞ + ＜鼠标左键＞ 在该规则的编号上点一下即可转换选取的动作。
2. 如果在编辑应用层防火墙时，某条规则呈现淡黄色背景时，代表您已选取该条规则。如果您希望透过筛选工具栏套用选定的政策在所有的通讯协议上时，请将鼠标移到第一条规则上，按鼠标左键往下拉，当所有规则的背景都呈现淡黄色时，代表所有规则已被选取。
3. 如果您要选取排列不连续的规则，您可以按住 ＜Ctrl＞，然后透过鼠标在选取的规则上点一下即可。

第7部

实时通讯管理员

第11章
自定义警告讯息

11.1 需求

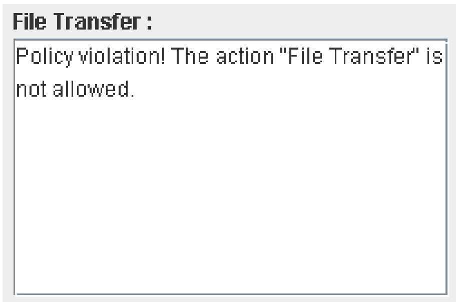
管理人员希望自定义符合实时通讯行为的警告讯息，当用户违反实时通讯政策，并实时在实时通讯窗口内收到警告讯息时才可从警告讯息的内容中得知自己的行为违反了哪条政策规则。

11.2 方法

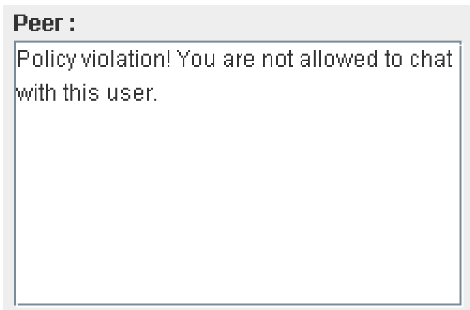
到 **Functions > Management > IM Manager > Message** 中编辑警告讯息。

11.3 步骤

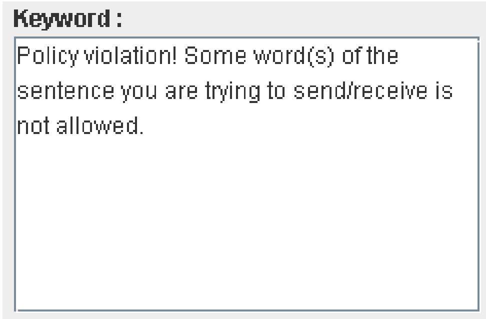
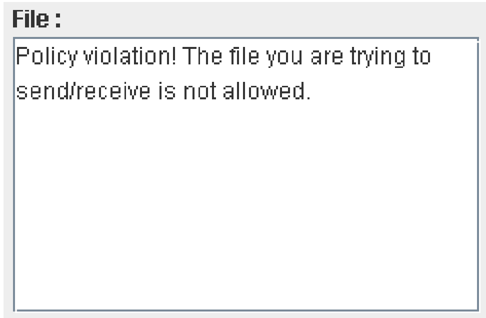
11.3.1 实时通讯服务

步骤 1 违反档案传送规则之警告讯息 编辑用户违反文件传输规则时，系统会在实时通讯窗口内发送给用户的警告讯息。 其余违反实时通讯服务的警告讯息编辑原则一样。	**Functions > Management > IM Manager > Message > IM Service** 

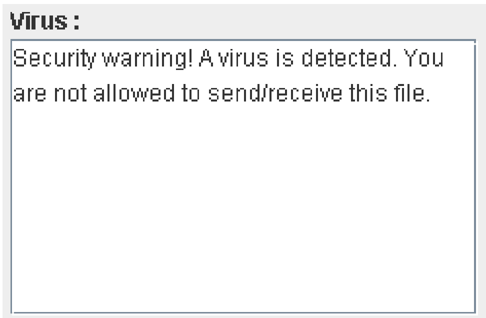
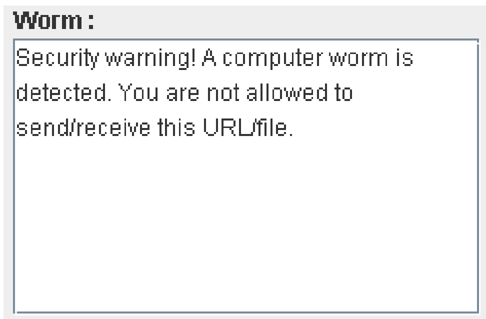
11.3.2 实时通讯聊天对象

步骤 1 违反聊天对象规则之警告讯息 编辑用户违反实时通讯聊天对象规则时，系统会在实时通讯窗口内发送给用户的警告讯息。	**Functions > Management > IM Manager > Message > IM Peer** 

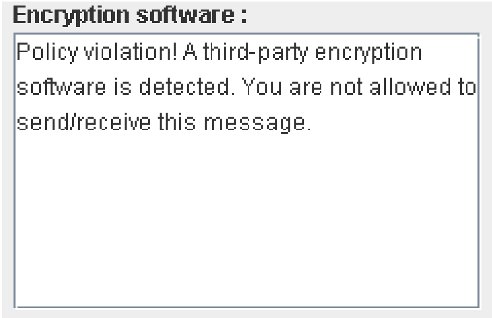
11.3.3 实时通讯内容

步驟 1 关键词拦阻 编辑传送不合法的关键词时，系统会在实时通讯窗口内发送给用户的警告讯息。	**Functions > Management > IM Manager > Message > IM Content** 
步驟 2 档案拦阻 编辑传送不合法的档案时，系统会在实时通讯窗口内发送给用户的警告讯息。	**Functions > Management > IM Manager > Message > IM Content** 

11.3.4 实时通讯病毒防护

步驟 1 病毒拦阻 编辑传送/接收的档案内如果藏匿有病毒，系统会在实时通讯窗口内发送给用户的警告讯息。	**Functions > Management > IM Manager > Message > IM Security** 
步驟 2 计算机蠕虫拦阻 编辑传送/接收的URL/档案内如果藏匿有计算机蠕虫，系统会在实时通讯窗口内发送给用户的警告讯息。	**Functions > Management > IM Manager > Message > IM Security** 

11.3.5 其余加密软件

<table>
<tr><td>步驟 1 拦阻加密软件
编辑当用户透过第三方加密软件聊天，被拦阻时，系统在实时通讯窗口显示给用户的讯息。</td><td>Functions > Management > IM Manager > Message > Others

</td></tr>
<tr><td colspan="2">步驟 2 上传配置文件
选择 Upload Configuration 或者点击图示 ，将现行的配置文件上传到装置上。</td></tr>
</table>

注意：

所谓第三方加密软件就是非由正规实时通讯软件如 MSN/Yahoo/ICQ/AOL 官方网站所提供，但可与其兼容的软件。当您启用 IM Manager 时，这些第三方加密软件就会被限制不可使用。

第12章 实时通讯服务/群组

12.1 需求

1. 网管人员希望依照工具性质来定义每位员工的实时通讯行为之权限。
2. 所有员工将依工作性质分成许多不同的群组，以方便网管人员控管其网络之使用。

12.2 方法

1. 定义实时通讯服务，让管理者可以视使用者需求为其选择适当的服务。
2. 将每个员工分配到其适合的群组中。

12.3 步骤

12.3.1 实时通讯服务

步骤 1 默认实时通讯服务

默认实时通讯服务如右图所示。你可依照您的需求修改或删除默认服务规则。

注意，如果某条实时通讯服务规则已被其他规则使用了，您不可以直接删除此规则，如欲删除，请先删除所有已包含此服务规则的其他规则。

Functions > Management > IM Manager > IM Services



步骤 2 新增实时通讯服务

将鼠标移到实时通讯服务上右键单击，然后点选 New Service。

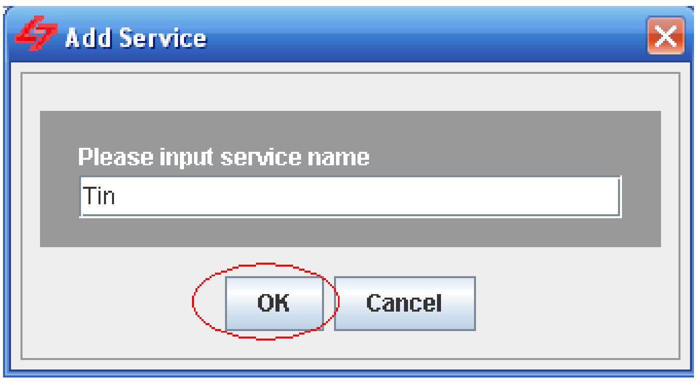
Functions > Management > IM Manager > IM Services



步骤 3 输入新服务名称

输入新增服务的名称，然后点击 **OK** 关闭窗口。

Functions > Management > IM Manager > IM Services



步驟 4 开启适用此规则的实时通讯行为

新增的实时通讯服务规则默认为禁止所有实时通讯行为，所以当您新增一条规则即要调整其默认设定。

将鼠标移到您要开启的项目上点一下，待图示 ✅ 出现即可。

Functions > Management > IM Manager > IM Services



步驟 5 启用实时通讯使用行为

启用 Login、FileTransfer、与 Voice。

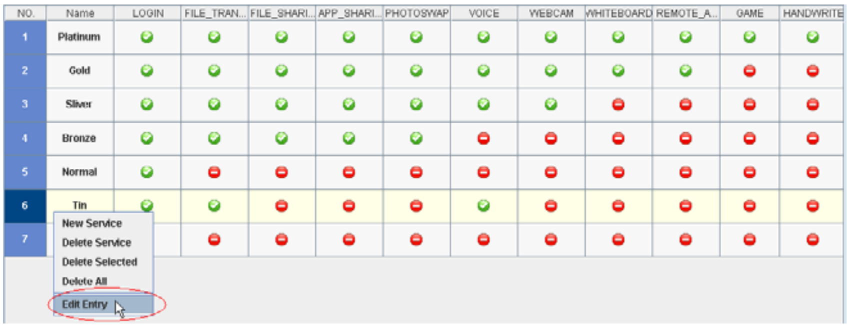
Functions > Management > IM Manager > IM Services



步驟 6 变更实时通讯服务规则名称

在选取的规则上右键单击，然后点选 **Edit Entry**。

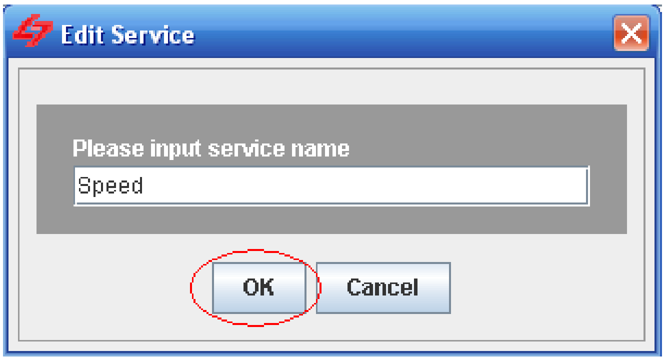
Functions > Management > IM Manager > IM Services



步驟 7 编辑服务名称

输入您要修改的服务名称，点击 **OK** 关闭窗口。

Functions > Management > IM Manager > IM Services



步驟 8 删除服务

将鼠标移到要删除的服务规则上右键单击，点选 Delete Service 或 Delete Selected 即可删除此服务。

Functions > Management > IM Manager > IM Services



步驟 9 上传配置文件到装置上

选择 **Upload Configuration** 或者点击图示  ，将现行的配置文件上传到装置上。

实时通讯使用行为	说明
登入	允许用户登入实时通讯软件与其他实时通讯用户在线传送讯息。
档案传送	允许实时通讯用户与其他用户传送或接收档案。
档案分享	允许实时通讯用户与其他用户分享档案。
应用程序分享	允许实时通讯用户与其他用户分享应用程序。
相片分享	允许实时通讯用户与其他用户分享相片。
语音	允许实时通讯用户与其他用户使用语音交谈。
影像	允许实时通讯用户与其他用户透过视讯交谈。
白板	允许实时通讯用户与其他用户透过白板书写笔记、画图或传送简讯。
远程协助	允许实时通讯用户与其他用户使用远程协助功能。
游戏	允许实时通讯用户与其他用户互相玩在线游戏。
手写	允许实时通讯用户透过手写功能传递讯息。

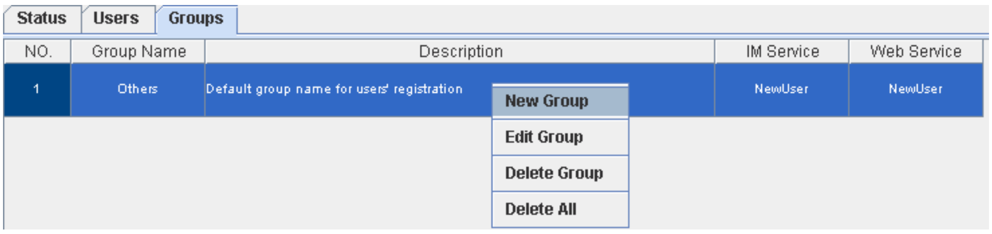
表格 12-1 可管理的实时通讯使用行为

12.3.2 实时通讯群组

步驟 1 自定义实时通讯群组

将鼠标移到实时通讯群组屏幕上右键单击，然后选择 New Group。命名此Group为Boss。

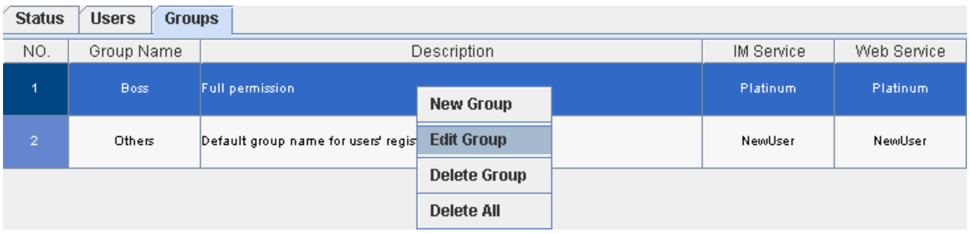
Functions > Console > User Console



步驟 2 编辑群组说明

将鼠标移到 Boss 规则的说明字段上右键单击，然后选择 **Edit Entry**。

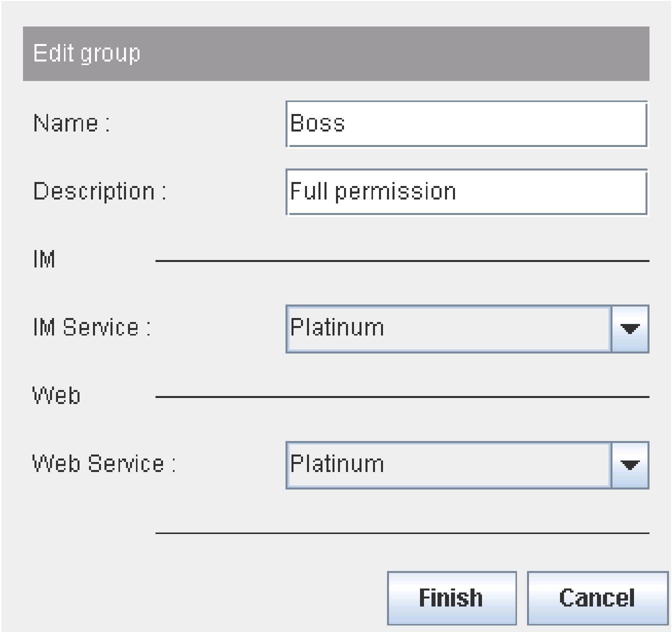
Functions > Console > User Console



步驟 3 输入群组说明

在 **Content** 字段内输入您要为此群组做的说明，然后点击 **OK** 继续。

Functions > Console > User Console



步驟 4 设定此群组的预设服务

选择此群组的预设服务。当实时通讯使用规则排程已过，系统将会套用默认规则于属于该群组的实时通讯用户上。

Functions > Console > User Console



步驟 5 上传配置文件

选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

注意：

除了手动建立实时通讯群组外，您也可以透过 AD Import 或者 File Import 的方式，从既有的数据库中汇入群组数据。请参阅以下章节。

第13章
实时通讯用户设定

13.1 需求

1. 实时通讯用户必须与现有的 AD 数据库整合。
2. 在上班时间，员工只可以使用 MSN，且需要被侧录存证，其余实时通讯软件一率禁止。员工可以选择使否要收到违反规则之警告信件。
3. 管理者想将已设定好的实时通讯用户备份存盘。

13.2 方法

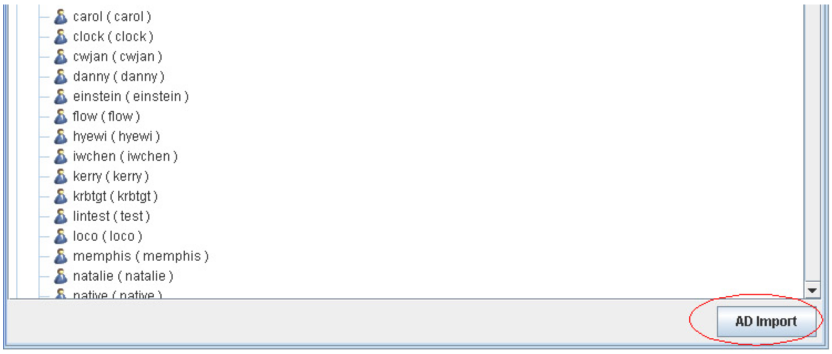
1. 从已存在的数据库中汇入实时通讯用户。
2. 将实时通讯使用规则默认为”Block”，上班时间只可以使用 MSN。每笔聊天记录都需要被侧录，且当用户违反规则时将收到警告信件。
3. 选择”File Export”将编辑好的实时通讯用户导出储存成档案。

13.3 步骤

当您启用实时通讯管理员，并上传设定文件到 InstantScan 装置上时，实时通讯用户立即受 InstantScan 控管。当您设定寄送警告信件给违反规则的用户时，用户将随时被知会其是否违反了公司的政策规则。InstantScan 提供您三个方法来编辑实时通讯用户的列表：1） 从现存的 AD 服务器汇入用户数据；2） 将现有数据库导出的文本文件汇入用户数据；3） 手动自行编辑用户清单。

管理者可以自行定义默认用户的行为模式为拦阻或是允许通行。以下的范例，将介绍您如何设定实时通讯用户。

13.3.1 AD Import – Open LDAP

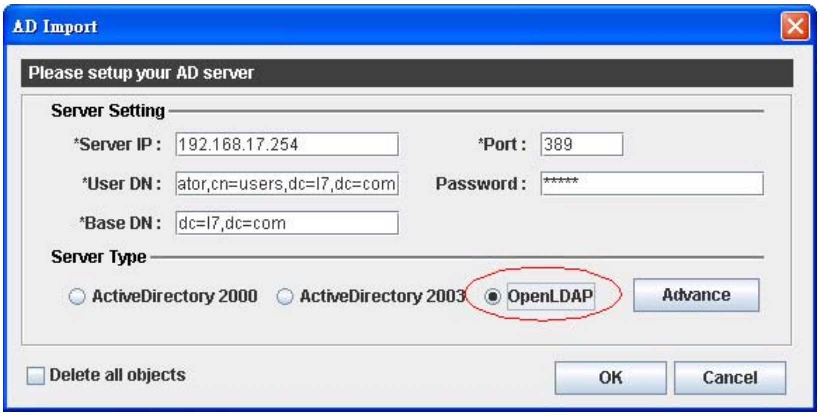
步驟 1 选择透过 AD 汇入用户数据 点击 **AD Import** 继续。	**Functions > Management > Object Manager > AD > AD Import** 

步驟 2 从 **OpenLDAP** 汇入

在服务器设定区域内，输入服务器 IP、端口（预设 = 389）、与您用来连结 OpenLDAP 服务器的 User DN 与密码。然后输入用户数据所在的 Base DN。圈选 OpenLDAP 为服务器类型。相关 Open LDAP 的设定，请参考章节 **錯誤! 找不到參照來源。** 与 **錯誤! 找不到參照來源。**。

请注意，打星号的字段为必填字段。

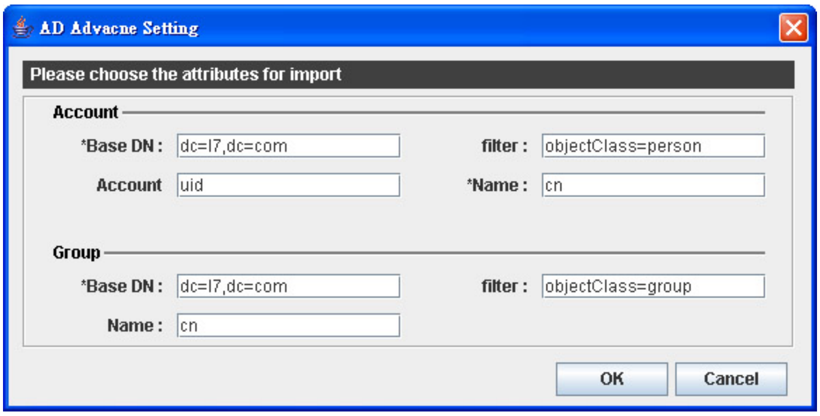
Functions > Management > Object Manager > AD > AD Import



步驟 3 **OpenLDAP** 进阶设定

进阶设定的筛选功能可让您更精确的汇入您需要的数据。有关 LDAP 进阶设定，请参考章节 **錯誤! 找不到參照來源。**。

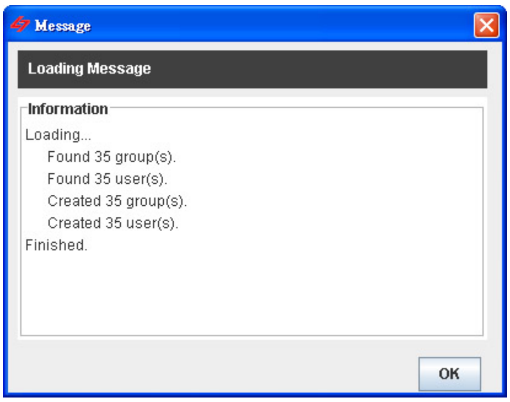
Functions > Management > Object Manager > AD > AD Import



步驟 4 汇入成功

当从LDAP服务器汇入数据成功，系统将会显示如右图的讯息告诉您。点击 **OK** 完成设定。

Functions > Management > Object Manager > AD > AD Import



步驟 5 上传配置文件

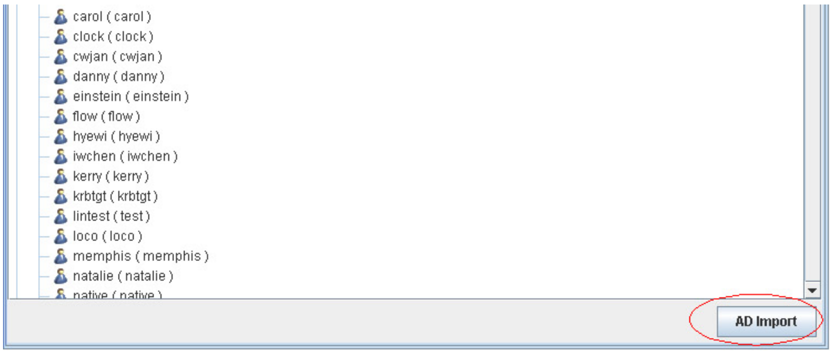
选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

13.3.2 AD Import – ActiveDirectory

步驟 1 选择透过 AD 汇入用户数据

点击 **AD Import** 继续。

Functions > Management > Object Manager > AD > AD Import



步驟 2 从 ActiveDirectory 汇入

在服务器设定区域内，输入服务器 IP、端口（预设 = 389）、与您用来连结 ActiveDirectory 服务器的 User DN 与密码。然后输入用户数据所在的 Base DN。圈选 ActiveDirectory 2003 为服务器类型。相关 ActiveDirectory 的设定，请参考章节 **錯誤! 找不到參照來源。** 与 **錯誤! 找不到參照來源。**。

请注意，打星号的字段为必填字段。

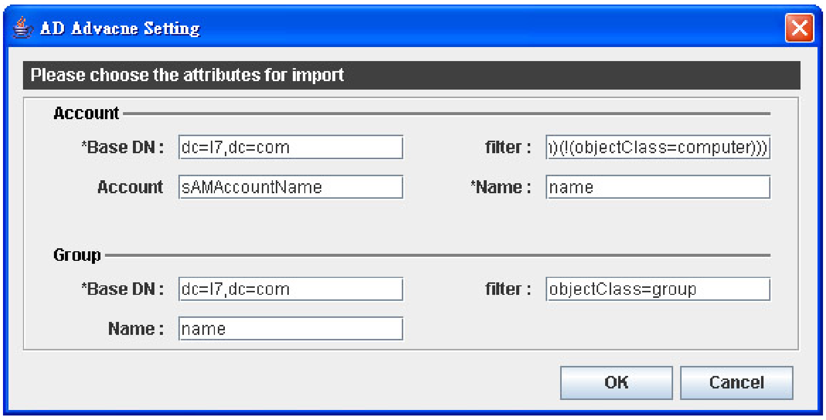
Functions > Management > Object Manager > AD > AD Import



步驟 3 ActiveDirectory 进阶设定

进阶设定的筛选功能可让您更精确的汇入您需要的数据。有关 LDAP 进阶设定，请参考章节 **錯誤! 找不到參照來源。**。

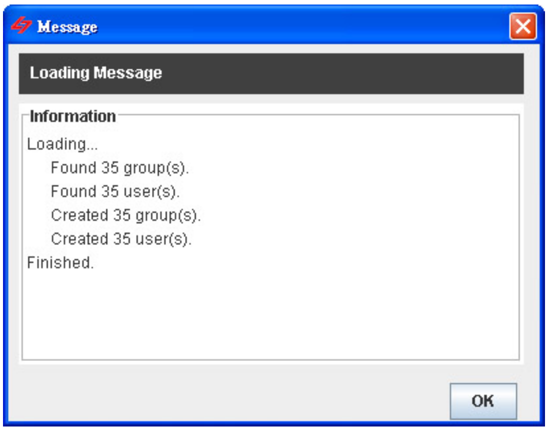
Functions > Management > Object Manager > AD > AD Import



步驟 4 汇入成功

当从 AD 服务器汇入数据成功，系统将会显示如右图的讯息告诉您。点击确定完成设定。

Functions > Management > IM Manager > IM User > LDAP Import



步驟 5 上传配置文件

选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

字段	说明	**ActiveDirectory 范例**	**Open LDAP 范例**
Server Setting			
Server IP	LDAP 服务器的 IP 地址	10.17.17.3	10.17.17.3
Port	LDAP 服务器数据进出的端口。	389 （预设）	389 （预设）
User DN	User DN 为授权用来存取 LDAP 服务器的资源。相当于使用者的账号。	Administrator	cn=manager,dc=yourCompany,dc=com
Password	用户存取 LDAP 服务器所需的密码。	ADLdapABC	OpenLDAP
Base DN	Base DN 为 LDAP 服务器上查询用户所需的路径目录。	cn=users,dc=ABC,dc=com	ou=people,dc=ABC, dc=com
Server Type			
ActiveDirectory 2002			
ActiveDirectory 2003			
OpenLDAP			
Advance			
Account			
Base DN	Base DN 是你在 AD 所建立组织的名字，如 ou=group,dc=ABC,dc=com。而这些都是你在安装的过程中，在设定 AD 时所做的设定。	cn=users,dc=yourCompany, dc=com	ou=people,dc=yourCompany, dc=com
filter	如果您想要汇入某个用户的资料，您可以透过这个过滤器来搜寻您要的数据。（ObjectClass=person）	(&(objectClass=person)(!(objectClass=computer)))	objectClass=person
Account	在此的名称是 LDAP 服务器上用来辨识使用者的账号字段。	sAMAccountName	uid
Name	在此的名称是 LDAP 服务器上用来辨识使用者的名称字段。	name	cn
Group			
Base DN	Base DN 是你在 LDAP 所建立组织的名字，如 ou=group,dc=ABC,dc=com。而这些都是你在安装的过程中，在设定 LDAP 时所做的设定。	cn=manager,dc=ABC,dc=com,dc=tw	ou=group,dc=ABC,dc=com
filter	如果您想要汇入某个用户的资料，您可以	objectClass=group	objectClass=group

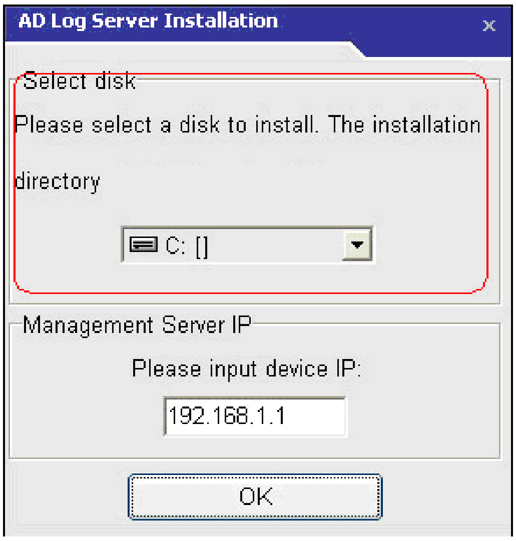
	透过这个过滤器来搜寻您要的数据。（ObjectClass=person）		
Name	在此的名称是 LDAP 服务器上用来辨识使用者群组的名称字段。	name	cn

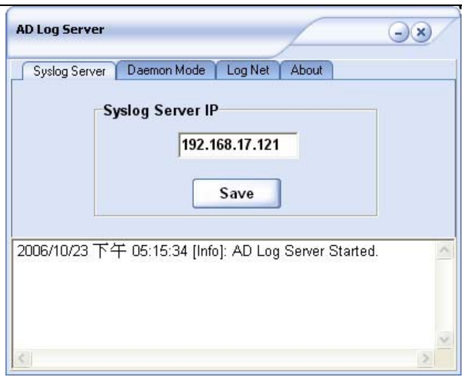
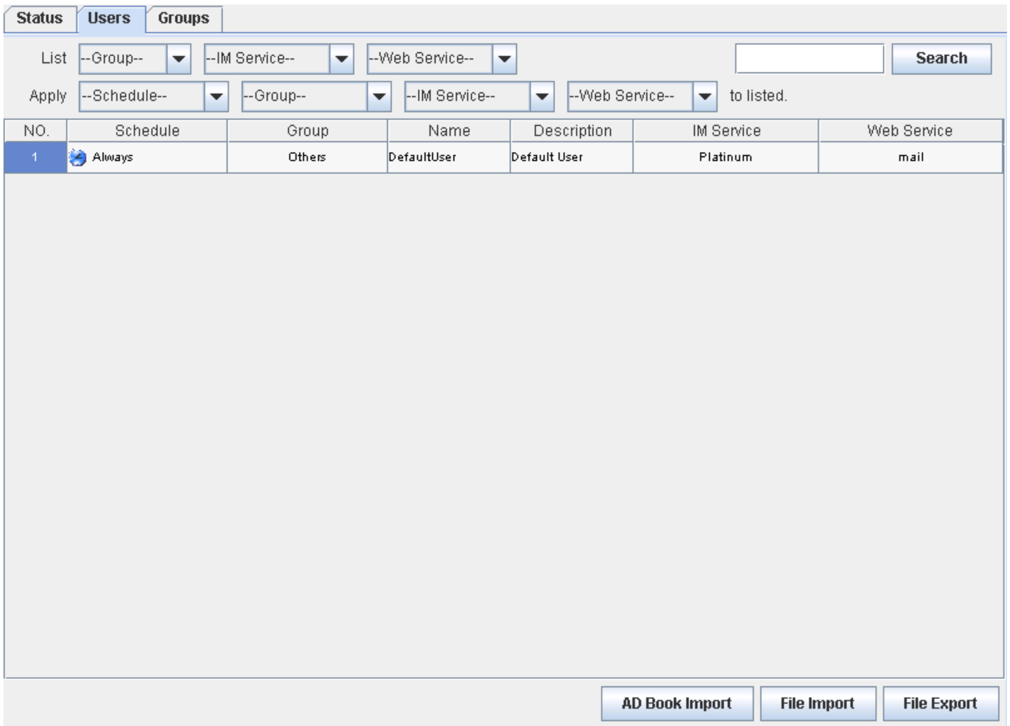
13.3.3 使用 AD Book Import

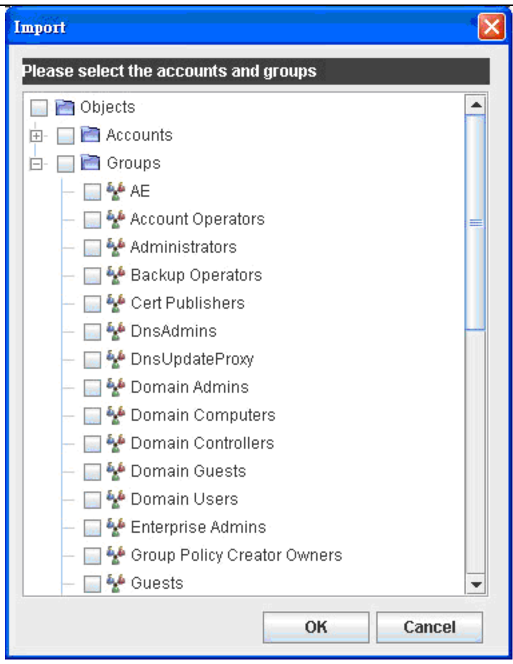
IM Manager 可以搭配 **AD Server** 自动从 **AD Server** 汇入使用者的账号与群组作管理。

安装程序概述：

- 安装 AD Log Server
- 启动 AD Manager(选购)
- AD Book Import…

步驟 1 安装 AD Log Server 启动本软件得安装程序 Setup.exe，点选 AD Log Server。	**安装接口 > AD Log Server**
步驟 2 设定安装路径与设定 device IP 选择 AD Log Server 要安装到那里。选将 IP 设定为跟设备的 IP 相同。 请注意：此 IP 设定的意思为 AD Log Server 是将 Log 送到那台 device 的意思。	**安装接口 > AD Log Server > AD Log Server Installation** 
步驟 3 安装完成 安装完成后会出现完成的讯息，点选确定即可。	**安装接口 > AD Log Server > AD Log Server Installation > Install completed** 
步驟 4 AD Log Server 设定 点选确定后会出现 AD Log Server 的设定接口。 第 1 页为 Syslog Server，可以改变步骤 3 所设定的值，按 Save 储存设定。 请注意：此 IP 设定的意思为 AD Log Server 是将 Log 送到那台 device。如果此窗口已被关闭，用	**Install completed > AD Log Server Setting**

户想再开启时，可到安装路径(本范例)下的 C:\L7Networks_AD 下启动 AD.exe 檔即可。	
步驟 5 开启 AD Manager 设定接口 此功能为选购功能，必须到本关网注册选购，再到 Management 操作接口开启即可使用(Update > License 输入所得到的 License Key)。完成开启后 Management 会出现 AD Manager 与 Encapsulation Manager 两种选项。	
步驟 6 AD Book Import 点选 AD Book Import 则会跳出 Import 的窗口。	**Functions > Management > IM Manager > IM User > AD Book Import** 
步驟 7 将 AD 账号汇入 点选想汇入的账号与群组，点选 OK 后即可。	**Functions > Management > IM Manager > IM User > AD Book Import**

请注意：请先完成 13.3.1 的相关操作后，此窗口内才会出现 AD 账号与群组。	
步骤 8 上传档案 选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。	

问题： 当 RD_1 为 RD Group 的一员，但是此两个账号同时出现在 IM User 时，配置文件该以谁为主?
解答： 配置文件的比对规则 IM account > AD User > AD Group > Default User

13.3.4 从本地端档案加载实时通讯用户与其群组

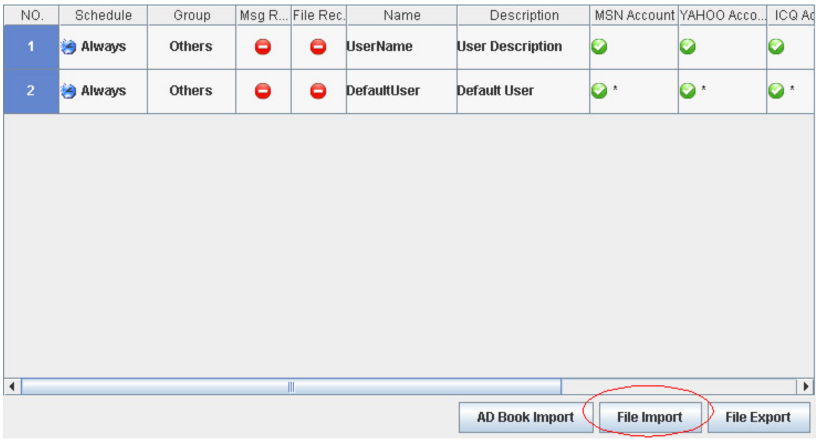
如果贵公司不支持 LDAP 汇入的方式，您可以将既有的数据库按照实时通讯用户的字段排列方式将数据导出并存成纯文本文件，然后藉由档案汇入的方式将实时通讯用户的数据汇入。

步骤 1 可汇入的纯文本档
您从既有的数据库导出的文本文件必需依据右图的格式，字段与字段间要用逗号分开。请注意，名称是主键，不可重复，所以在您透过档案汇入用户数据前，请检查数据是否有重复、字段是否符合要汇入的目标字段。
	Functions > Management > IM Manager > IM User > File Import
	`ceo, boss, ceo@yourCompany.com, ceo@hotmail.com, ceo1111`
	`cto, boss, cto@yourCompany.com, cto@hotmail.com, cto1010`

步驟 2 汇入档案数据

点击 File Import 继续。

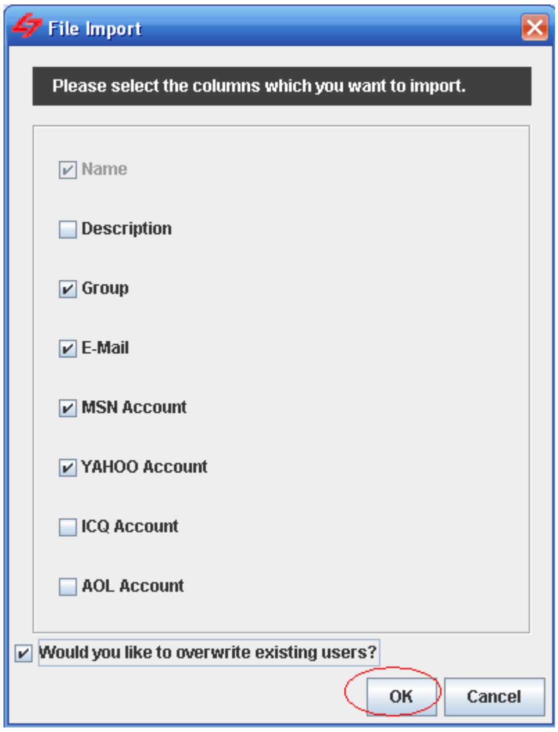
Functions > Management > IM Manager > IM User > File Import



步驟 3 选择要汇入的字段

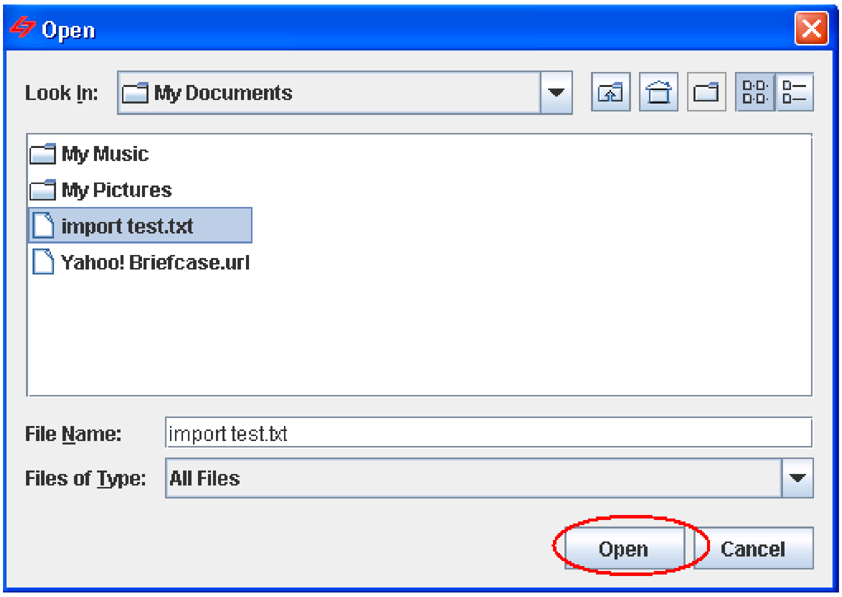
勾选 Group、E-Mail、MSN Account、Yahoo Account，然后勾选 **Would you like to overwrite existing users?** 覆写已存在的使用者，点击 **OK** 进入下一个窗口。

Functions > Management > IM Manager > IM User > File Import



步驟 4 选择要汇入的档案

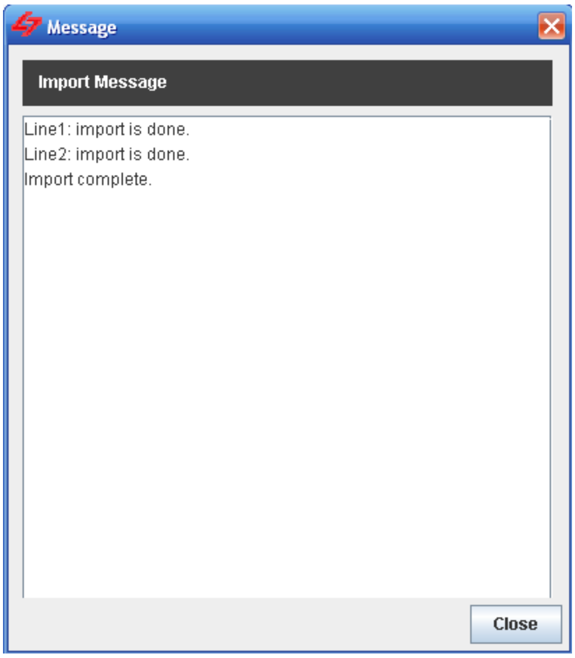
选择您要汇入的文本文件，然后点击 **Open** 开始汇入动作。



步驟 5 汇入成功

当档案汇入数据成功后，系统将会显示如右图的讯息告诉您汇入成功。点击 **Close** 完成设定。

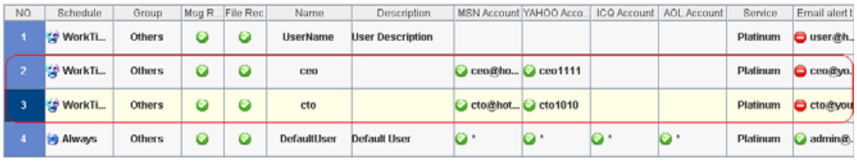
Functions > Management > IM Manager > IM User > File Import



步驟 6 显示档案汇入的结果

当汇入数据后，您可以在本页检视汇入结果。请注意，汇入的数据其设定都是默认值，网管人员必须视情况调整每位实时通讯用户的规则。

Functions > Management > IM Manager > IM User



NO.	Schedule	Group	Msg R...	File Rec.	Name	Description	MSN Account	YAHOO Acco...	ICQ Account	AOL Account	Service	Email alert t
1	WorkTi...	Others			UserName	User Description					Platinum	user@h...
2	WorkTi...	Others			ceo		ceo@ho...	ceo1111			Platinum	ceo@yo.
3	WorkTi...	Others			cto		cto@hot...	cto1010			Platinum	cto@you
4	Always	Others			DefaultUser	Default User	*	*	*	*	Platinum	admin@.

步驟 7 上传配置文件

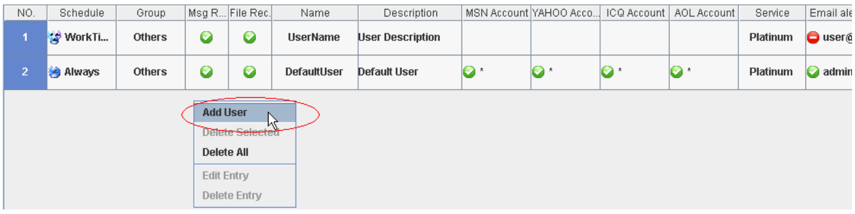
选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

13.3.5 手动编辑实时通讯用户

步驟 1 新增实时通讯用户

在 IM User 窗口上右键单击，然后选择 Add User。

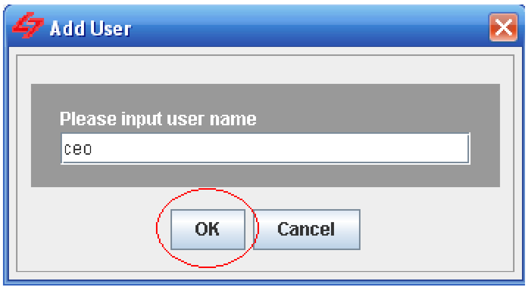
Functions > Management > IM Manager > IM User



步驟 2 输入使用者名称

输入实时通讯用户的规则名称。点击 **OK** 关闭窗口。

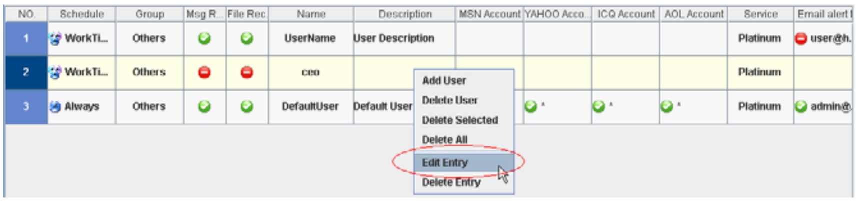
Functions > Management > IM Manager > IM User



步驟 3 编辑使用者描述

在 Description 字段上右键单击，然后选择 **Edit Entry**。

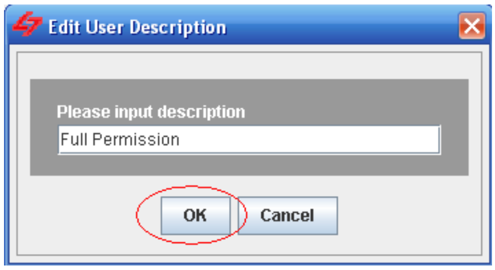
Functions > Management > IM Manager > IM User



步驟 4 输入描述字段内容

输入针对此使用者的描述内容。点击 **OK** 结束窗口。

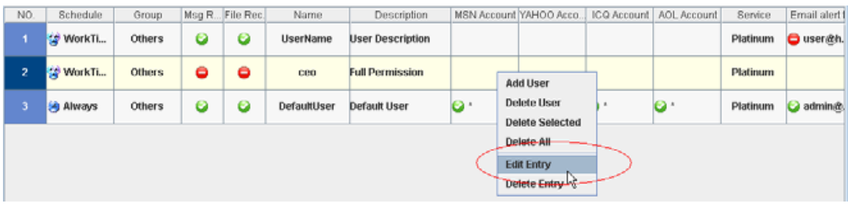
Functions > Management > IM Manager > IM User

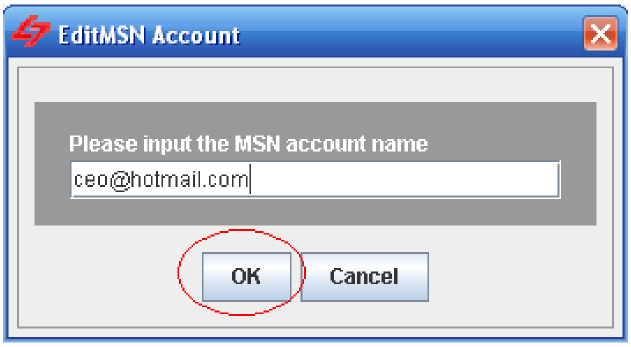
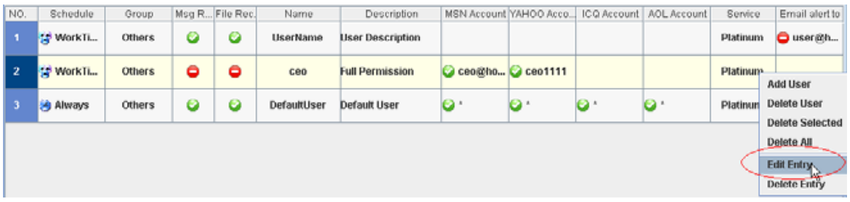
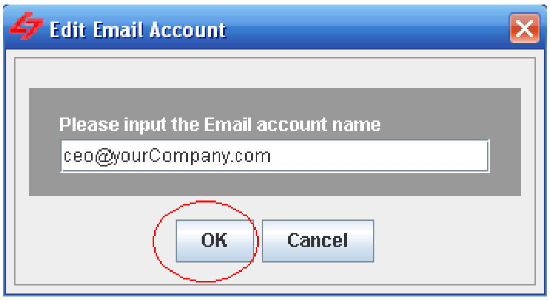


步驟 5 编辑用户的实时通讯账号

在 MSN Account 字段上右键单击，然后选择 **Edit Entry**。

Functions > Management > IM Manager > IM User



步驟 6 输入用户的实时通讯账号 在 Account 字段内输入此使用者的 MSN 账号。 其余实时通讯账号设定步骤同 MSN 账号。	**Functions > Management > IM Manager > IM User** 
步驟 7 编辑警告信件信箱 在 Eamil alert to 字段上右键单击，然后选择 Edit Entry。	**Functions > Management > IM Manager > IM User** 
步驟 8 输入电子邮件信箱 输入要接收警告信件的电子邮件信箱。当您设定好此邮件信箱，并启用设定后，当此用户违反政策规则时，系统将会寄送警告信件给此使用者。	**Functions > Management > IM Manager > IM User** 
步驟 9 检视已编辑好的实时通讯用户 新增加的实时通讯用户的设定都是默认值，网管人员必须视情况调整每位实时通讯用户的规则。	**Functions > Management > IM Manager > IM User** 
步驟 10 上传配置文件 选择 **Upload Configuration** 或点击图示 将配置文件上传到装置上。	

Email alert to 的字段是让管理者可以设定是否要让用户在其违反政策规则时收到警告信件，了解自己是触犯哪条政策规则。如果管理者允许用户使用实时通讯，也就是说实时通讯账号是启用的状态 ，请详见下表的规则：

图示	字段	说明
(绿色)	Email alert to	当用户违反实时通讯政策时，将收到警告信件。
(红色)	Email alert to	当用户违反实时通讯政策时，将不会收到警告信件。

表格 13-1 实时通讯政策允许使用实时通讯软件

如果管理者不允许用户使用实时通讯，也就是说实时通讯账号是未启用的状态 ，请详见下表的规则：

图示	字段	说明
(绿色)	Email alert to	当实时通讯用户企图使用实时通讯行为，将会收到警告信件。
(红色)	Email alert to	实时通讯用户将不会收到任何实时通讯警告信件。

表格 13-2 实时通讯政策不允许使用实时通讯软件

字段	说明	范围/格式	范例
No	实时通讯用户的编号。数字越小代表优先权越高。因其为由上到下的比对法。	数字	2
Schedule	启用或取消实时通讯用户政策规则的时间。	Always / Never / 使用者定义	Always
Group	用户定义的实时通讯用户群组。	使用者定义	boss
Msg Rec.	实时通讯讯息侧录器。当您开启时，所有实时通讯讯息都会被侧录。	（启用） / （取消）	
File Rec.	实时通讯档案侧录器。当您开启时，所有实时通讯档案都会被侧录。	（启用） / （取消）	
Name	实时通讯用户规则名称。	使用者定义	ceo
Description	实时通讯用户的描述。	使用者定义	Full permission
MSN account	MSN 账号。	MSN 账号格式	ceo@hotmail.com
YAHOO account	Yahoo 账号。	Yahoo 账号格式	ceo1111
ICQ account	ICQ 账号。	ICQ 账号格式	--
AOL account	AOL 账号。	AOL 账号格式	--
Service	实时通讯使用行为权限。	使用者定义	Platinum
Email alert to	当实时通讯违反政策规则时，可接收警告信件的账号。	电子邮件账号格式	ceo@abc.com

表格 13-3 实时通讯用户字段说明

13.3.6 自动学习实时通讯用户名单

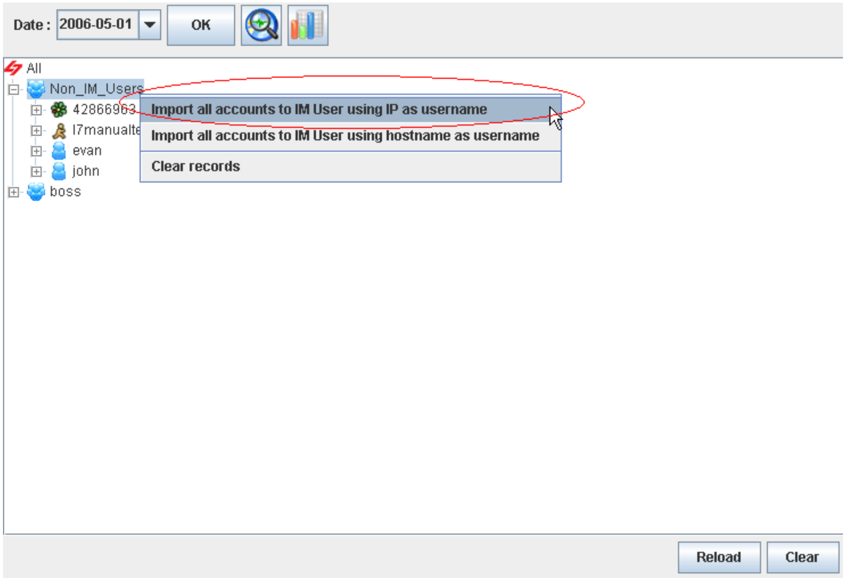
为了让管理者能够快速设定用户的实时通讯账号，设定了实时通讯账号自动学习的功能。管理者只要利用实时通讯记录器上侧录到的账号，即可右键单击选择账号汇入的方式即可。详细设定，请参照下表说明。

步驟 1 汇入所有使用者

在 Non_IM_Users （非 IM Users 清单上的账号）上右键单击，选择您要将实时通讯账号汇入的方式。

注意，已经加入的群组或实时通讯用户就不可以再次汇入账号了。也就是说，当您将 Non_IM_Users 的账号汇入 IM Users 列表内，则系统将会自动将该账号显示为 IM Users 上所设定的名称。记录器上所显示的树形图，第一层为群组、第二层为 IS 内部的实时通讯账号、第三层为该账号与其他账号之间的通讯记录。

Functions > Auditor > IM Recorder



字段	说明
Import all accounts to IM User using IP as username	将所有已记录的账号汇入实时通讯用户中，并以其传送/接收讯息者的 IP 为用户名称。
Import all accounts to IM User using hostname as username	将所有已记录的账号汇入实时通讯用户中，并以其传送/接收讯息者的主机名为用户名称。
Clear records	清除所有通讯记录。

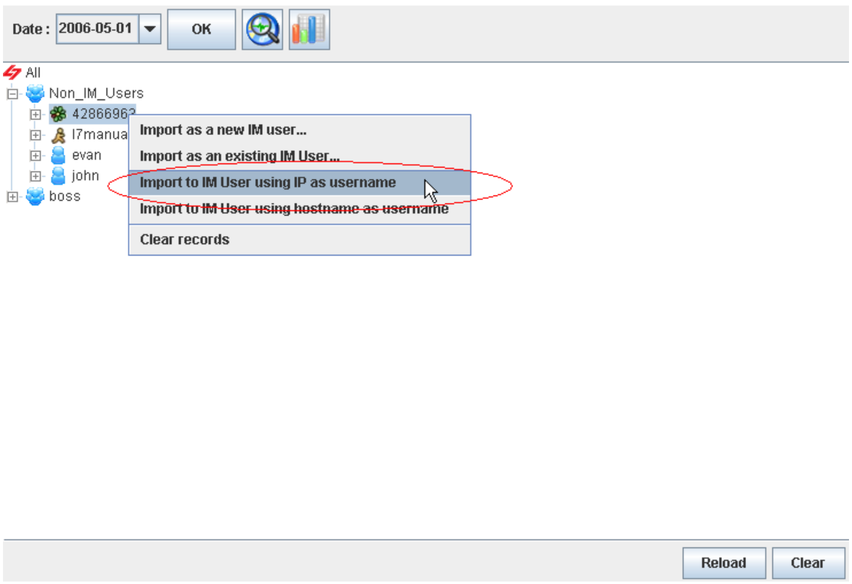
表格 13-1 自动账号学习 - 汇入所有非实时通讯用户列表上的账号

步驟 2 汇入选定的使用者

除了将所有账号汇入外，您也可以选定账号汇入。

在 Non_IM_Users 群组下，选择您要汇入的账号，然后在此账号上右键单击，选择您要将账号汇入的方式。相关说明请参考表格介绍。

Functions > Auditor > IM Recorder



Field	Description	Example
Import as a new IM user	将选定的实时通讯账号，以新增一笔新规则的	4286963

	方式汇入实时通讯用户列表内。	
Import as an existing IM User	将选定的实时通讯账号，汇入已存在的实时通讯用户列表内。	Evan
Import to IM User using IP as username	将选定的实时通讯账号，依其 IP 地址命名汇入实时通讯用户列表内。	192.168.168.10
Import to IM User using hostname as username	将选定的实时讯账号，依其主机名汇入实时通讯用户列表内。	ABC-Evan
Clear records	清除选定账号的所有记录。	--

表格 13-2 自动账号学习 - 汇入选定的非实时通讯用户列表上的账号

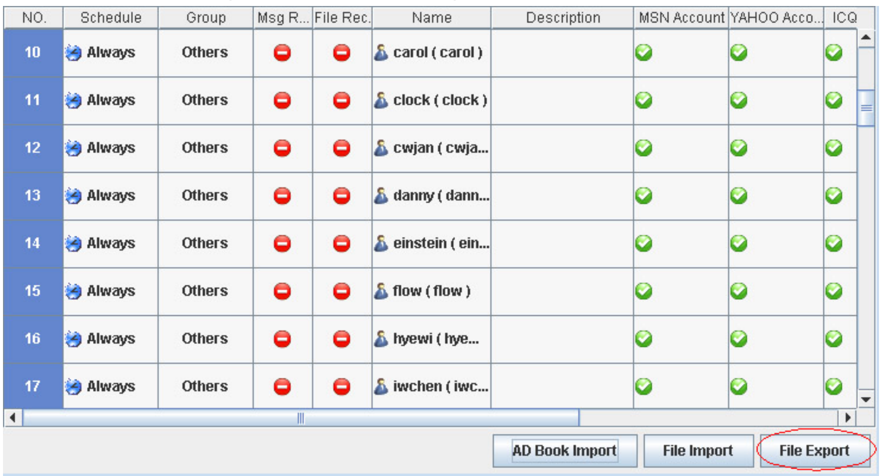
13.3.7 从本地端档案导出实时通讯用户与其群组

为了避免不可预期的因素，造成已设定好的实时通讯用户配置文件损毁，您可随时将实时通讯用户导出成档案储存，以备不时之需。

步驟 1 档案汇出

点击 File Export 导出实时通讯用户数据。

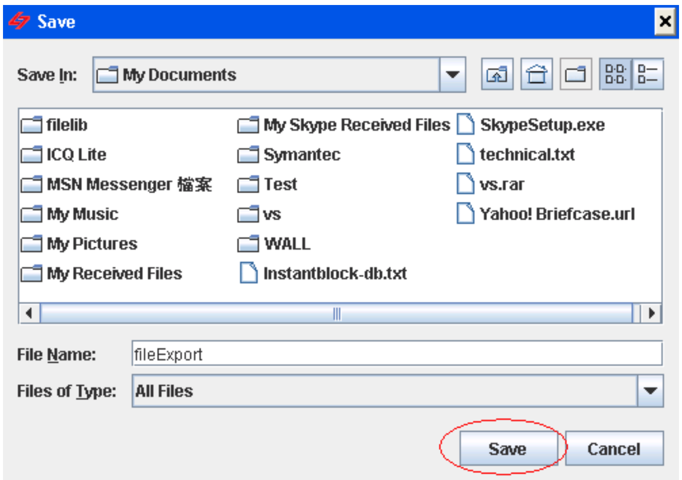
Functions > Management > IM Manager > IM User > File Export

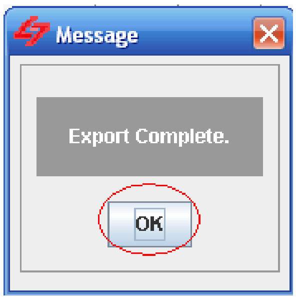


步驟 2 输入要储存的档案

在 File Name 字段内输入要储存的档案，然后点击 Save 储存。

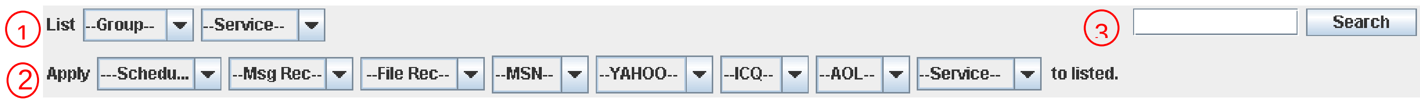
Functions > Management > IM Manager > IM User > File Export



步驟 3 汇出完成	**Functions > Management > IM Manager > IM User > File Export**
当档案汇出成功后，将有如右图的讯息告知您。请点击 **OK** 结束设定。	

13.3.8 实时通讯用户设定辅助工具栏

为了加速实时通讯用户的设定，InstantScan 提供下列设定辅助工具栏： **1**） 列举（**List**）选定的项目。所有选定的群组/服务将被列举在屏幕上。**2**） 套用（**Apply**）选定的项目到列举的实时通讯用户列表中。



字段		说明	范围 / 格式	范例
List ①	Group	列举选定的群组在实时通讯用户列表上。	使用者定义的群组	Boss
	Service	列举选定的服务在实时通讯用户列表上。	使用者定义的服务	--
Apply ___ to listed. ②	Schedule	套用选定的排程到列举的实时通讯用户列表上。	使用者定义的排程	Always
	Msg Rec.	套用选定的讯息侧录规则到列举的实时通讯用户列表上。	（启用） / （取消）	
	File Rec.	套用选定的档案侧录规则到列举的实时通讯用户列表上。	（启用） / （取消）	
	MSN	套用选定的 MSN 规则到列举的实时通讯用户列表上。	Block/Allow	Allow
	YAHOO	套用选定的 Yahoo 规则到列举的实时通讯用户列表上。	Block/Allow	Allow
	AOL	套用选定的 AOL 规则到列举的实时通讯用户列表上。	Block/Allow	Allow
	ICQ	套用选定的 ICQ 规则到列举的实时通讯用户列表上。	Block/Allow	Allow
	Service	套用选定的服务规则到列举的实时通讯使用	使用者定义的服务	Platinum
Search		此搜寻功能让您利用关键词快速寻找特定的规则。		

表格 13-4 实时通讯用户辅助设定工具栏

第14章 管理实时通讯用户

14.1 需求

1. 为了设定的方便，需要调整新增实时通讯用户的默认值。
2. 在上班时间，员工只可以使用 MSN，且需要被侧录存证，其余实时通讯软件一率禁止。当员工使用某些实时通讯软件被阻文件时，需要知道其违反了哪项政策规则。
3. 因工作性质关系，研发部 RD 在上班时间不准与公司外的人员聊天。
4. 所有传送的实时通讯讯息与档案都需要作内容过滤，避免员工利用实时通讯的便利在上班时间聊工作之外的事情与传送不必要的档案，浪费公司网络带宽。
5. 所有传送接收的档案都需要扫毒，以保护公司内部的计算机。
6. 因为管理部门的 CEO 与 CTO 有特殊的需求，所以不列入实时通讯管理员控管的范围。

14.2 方法

1. 在 Functions > Management > IM Manager > Status > New IM User Setting 页面上设定新增加的实时通讯用户默认值。
2. 在 Functions > Management > IM Manager > IM Users 页面设定实时通讯用户的政策。
3. 在 Functions > Management > IM Manager > IM Peers 页面设定 RD 群组不可以与 Non_IM_User 聊天。
4. 在 Functions > Management > IM Manager > IM Contents 页面设定要过滤的讯息与档案，并启用设定。
5. 在 Functions > Management > IM Manager > IM Security 页面启用防毒与防蠕虫功能。
6. 在 Functions > Management > IM Manager > Exempt Sources 页面设定，Boss（CEO/CTO）的联机都避开实时通讯管理员的控管。

14.3 步骤

14.3.1 新增的实时通讯用户默认值

<table>
<tr>
<td>

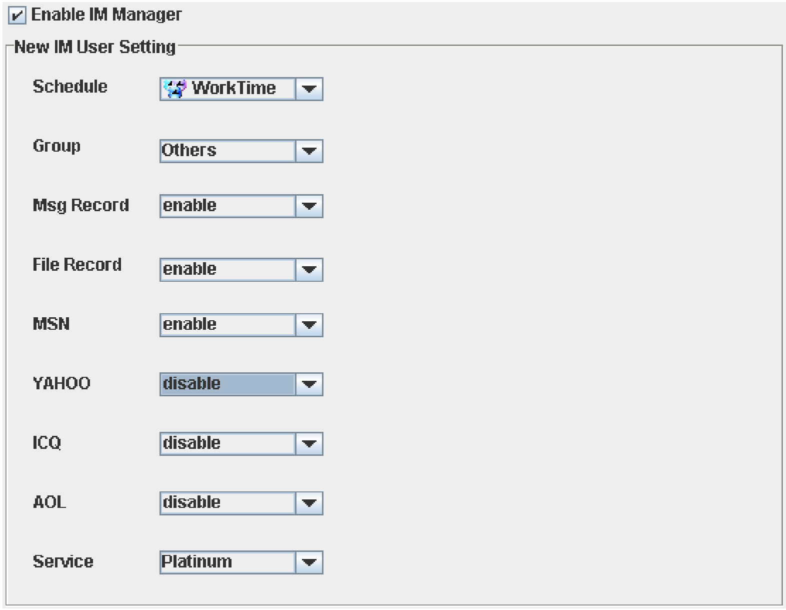
步驟 1 调整实时通讯用户默认值

为了配合实时通讯用户的政策，所以调整 New IM User 的设定值为：
Schedule: WorkTime
Group: Others
Msg Record: enable
File Record: enable
MSN: enable
YAHOO: disable
ICQ: disable
AOL: disable
Service: Platinum

当您设定好此默认值后，往后增加的实时通讯用户都会套用此设定。

</td>
<td>

Functions > Management > IM Manager > Status



</td>
</tr>
</table>

14.3.2 实时通讯用户管理

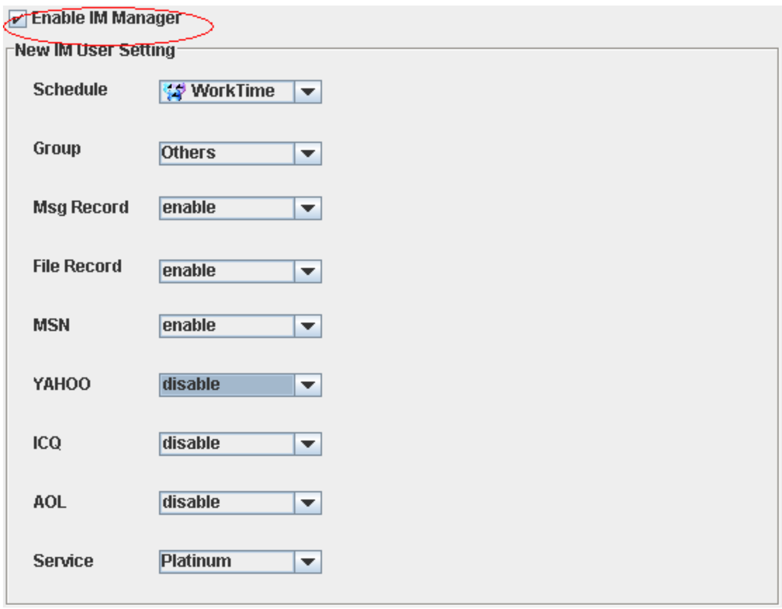
<table>
<tr>
<td>

步驟 1 启用实时通讯管理员

勾选 **Enable IM Manager**。

</td>
<td>

Functions > Management > IM Manager > Status



</td>
</tr>
</table>

步驟 2 允许使用 MSN，拦阻其他实时通讯

移动鼠标在 MSN Account 上点一下，让图示呈现（允许），然后让其他实时通讯软件的图标呈现（拦阻）。您亦可藉由 IM Users 窗口上的工具栏，快速设定实时通讯用户的政策。

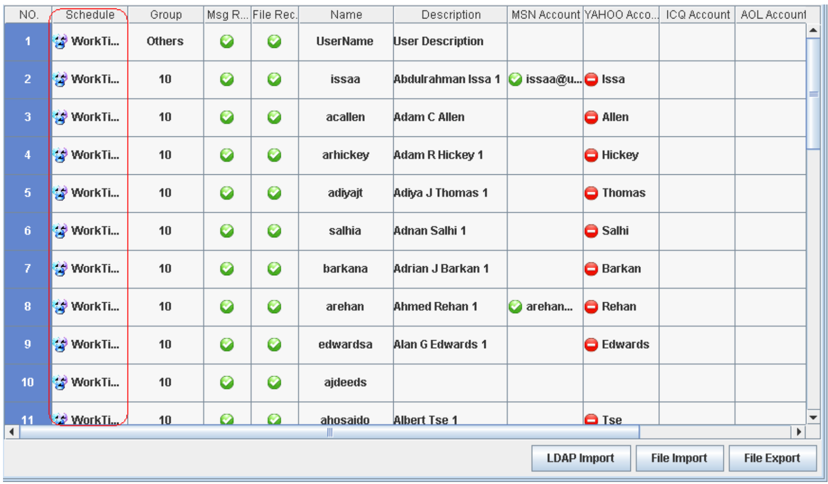
Functions > Management > IM Manager > IM Users



步驟 3 设定排程为 WorkTime

在前面的章节，我们已经介绍您如何设定 Schedule 了。请在 Schedule 字段上拉选 WorkTime。您亦可以利用 <ctrl> + 鼠标选择/取消您要套用的实时通讯用户，然后在工具栏上选择 Apply “WorkTime” to listed。

Functions > Management > IM Manager > IM Users



步驟 4 开启讯息/档案侧录功能

移动鼠标在 Msg Rec. 字段上点一下 开启讯息侧录与在 File Rec. 字段上点一下 开启档案侧录。然后在 Email alert to 字段上点一下 开启邮寄警告信件的服务。

注意：您也可以藉由 IM Users 窗口上的工具栏，快速设定实时通讯用户政策。

Functions > Management > IM Manager > IM Users



步驟 5 上传配置文件

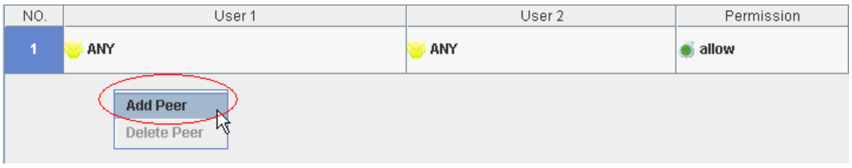
选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

14.3.3 实时通讯聊天对象管理

步骤 1 新增实时通讯聊天对象规则

将鼠标移到 IM Peer 的屏幕上右键单击，点选 Add Peer。

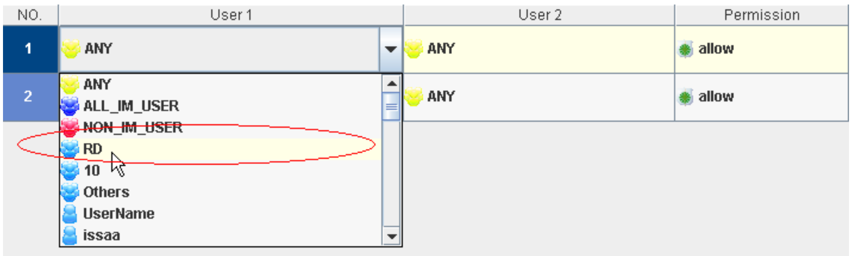
Functions > Management > IM Manager > IM Peer



步骤 2 选择 User1

在 User 1 字段上选择 RD。

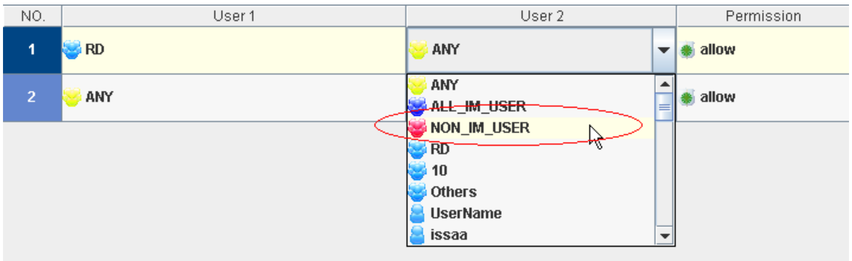
Functions > Management > IM Manager > IM Peer



步骤 3 选择 User2

在 User2 字段上选择 NON_IM_USER。

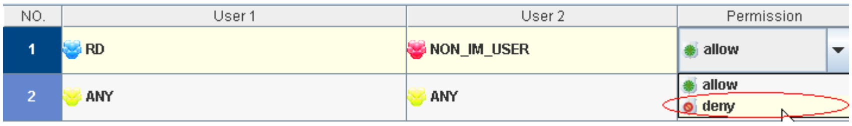
Functions > Management > IM Manager > IM Peer



步骤 4 拦阻 RD 与 NON_IM_User间的对话

在 Permission 字段上选择 deny。

Functions > Management > IM Manager > IM Peer



步骤 5 检视新增的实时通讯聊天对象规则

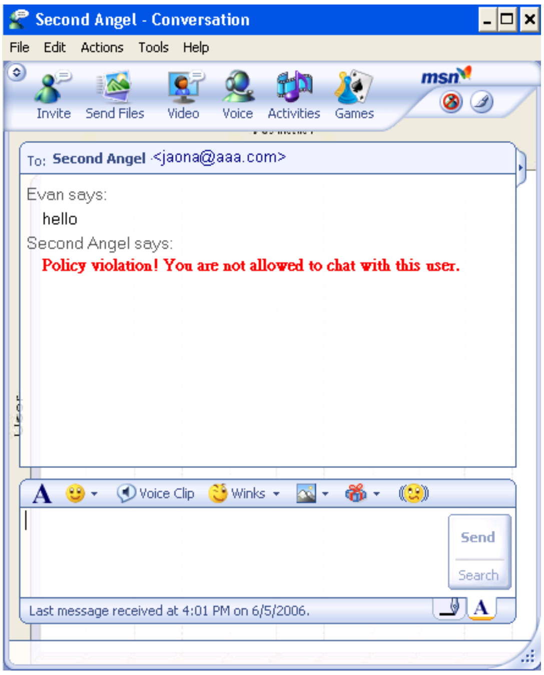
检视已新增的聊天对象规则。

Functions > Management > IM Manager > IM Peer



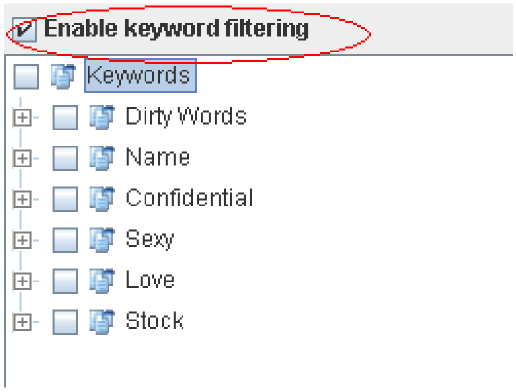
步骤 6 上传配置文件

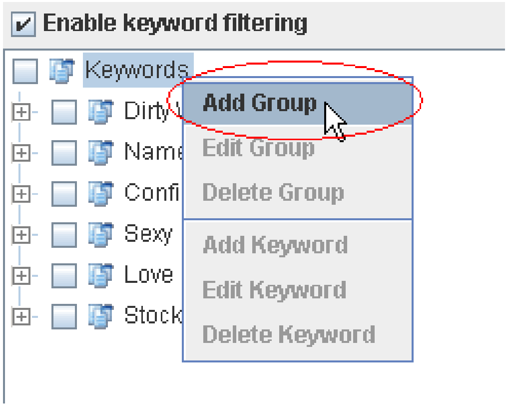
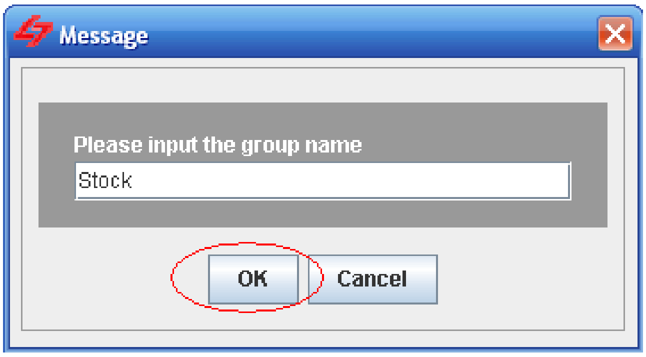
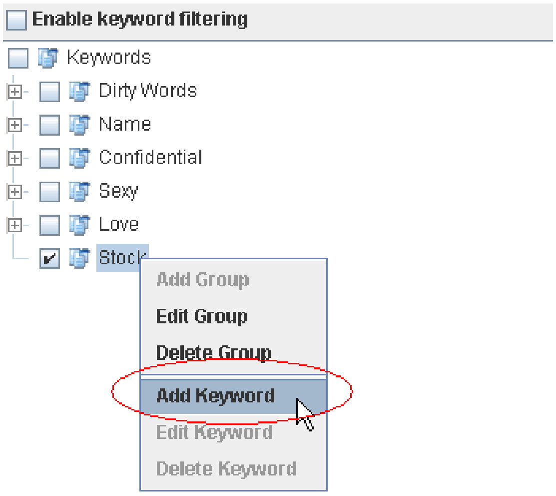
选择 **Upload Configuration** 或点击图示 将配置文件上传到装置上。

步驟 7 违反聊天对象警告讯息 当属于 RD 部门的 Evan 企图与非公司内部员工且已列举在 IM Users 清单上的用户聊天时，InstantScan 将拦阻他们之间的对话，且在实时通讯窗口显示如右图的警告。	

14.3.4 实时通讯内容过滤

14.3.4.1 关键词过滤

步驟 1 启用关键词过滤 勾选 **Enable keyword filtering**。	**Functions > Management > IM Manager > IM Contents > Chat** 

<table>
<tr>
<td>步驟 2 新增关键词
将鼠标移到 IM Contents > Chat 的屏幕上右键单击，点选 Add Group。</td>
<td>Functions > Management > IM Manager > IM Contents > Chat

</td>
</tr>
<tr>
<td>步驟 3 输入关键词组名
输入关键词组名，然后点击确定继续。</td>
<td>Functions > Management > IM Manager > IM Contents > Chat

</td>
</tr>
<tr>
<td>步驟 4 新增关键词
在刚刚新增的群组上右键单击，然后点选 Add Keyword。</td>
<td>Functions > Management > IM Manager > IM Contents > Chat

</td>
</tr>
</table>

步骤 5 输入关键词

输入需要内容过滤的关键词。

Functions > Management > IM Manager > IM Contents > Chat

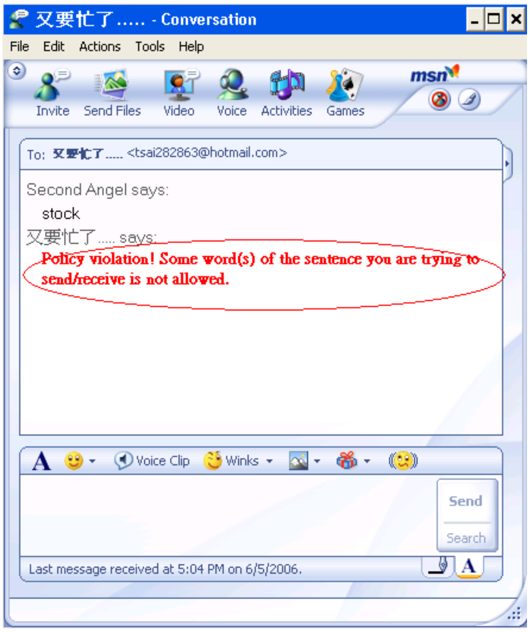


步骤 6 上传配置文件

选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

步骤 7 违反聊天关键词过滤警告讯息

当用户违反聊天关键词时，将如右图在实时通讯窗口内出现警告讯息。

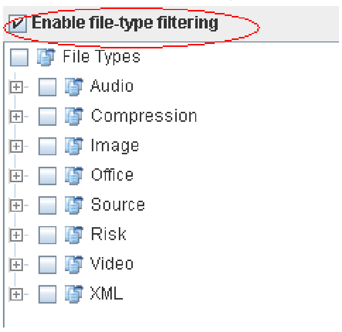


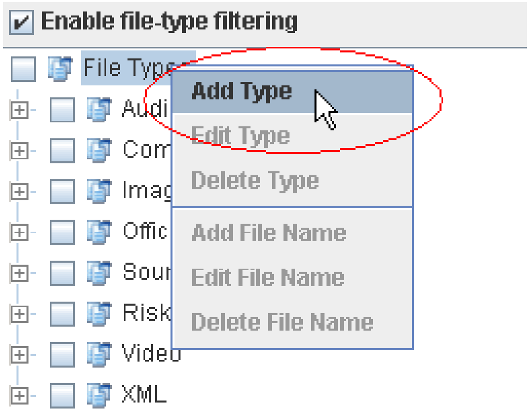
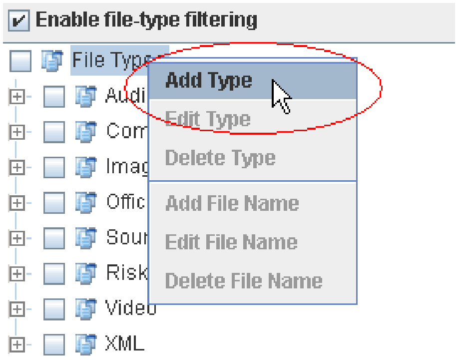
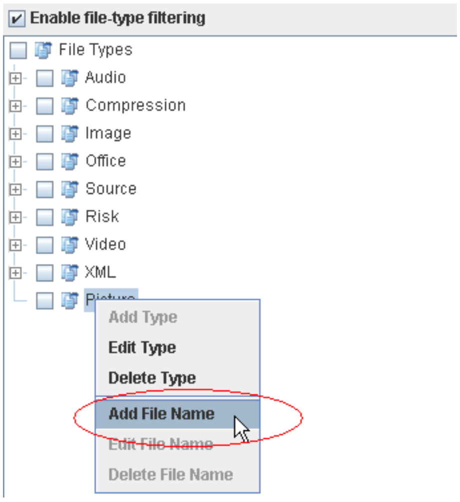
14.3.4.2 文件类型过滤

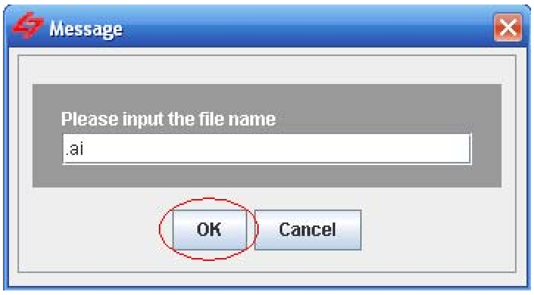
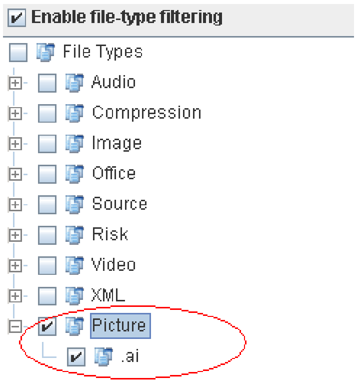
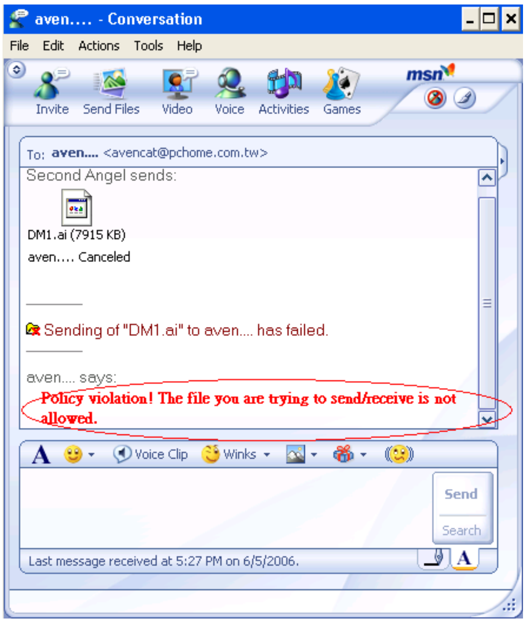
步骤 1 启用文件类型过滤

勾选 **Enable file-type filtering**。

Functions > Management > IM Manager > IM Contents > File

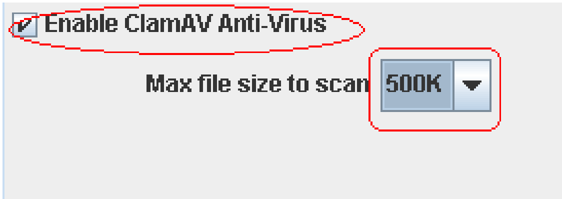
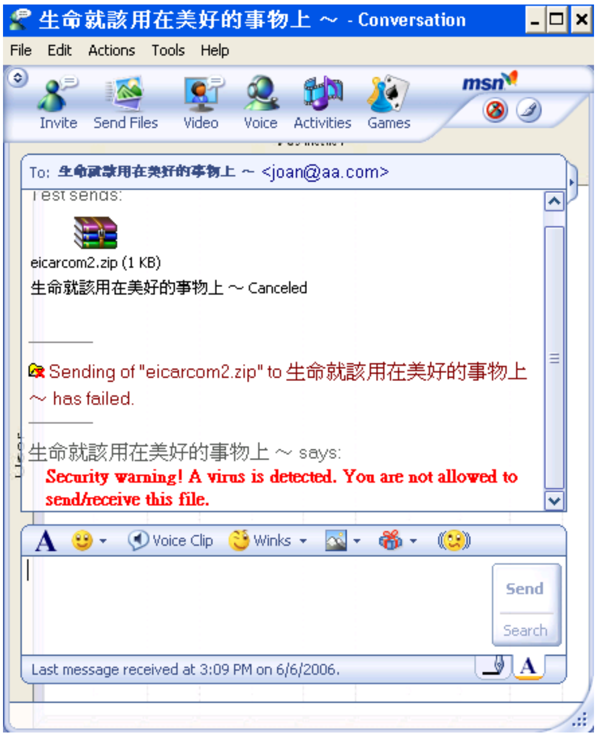


步驟 2 新增文件类型 将鼠标移到 IM Contents > File 的屏幕上右键单击，点选 **Add Type**。	**Functions > Management > IM Manager > IM Contents > File** 
步驟 3 输入文件类型 输入文件类型，然后点击**确定**继续。	**Functions > Management > IM Manager > IM Contents > File** 
步驟 4 新增文件名 在刚刚新增的文件类型上右键单击，然后点选 Add File Name。	**Functions > Management > IM Manager > IM Contents > File** 

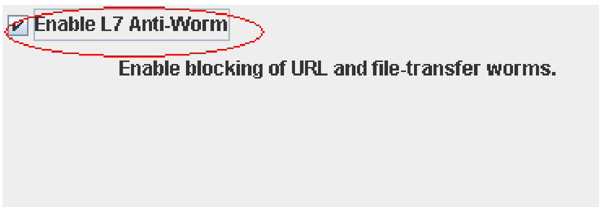
步驟 5　输入文件名 在此您可以输入扩展名如 .ai，系统将会过滤所有 .ai 类型的档案。	
步驟 6　启用文件类型过滤 勾选 **Enable file-type filtering**，并勾选刚刚新增的文件类型。	**Functions > Management > IM Manager > IM Contents > File** 
步驟 7　上传配置文件 选择 **Upload Configuration** 或点击图示 将配置文件上传到装置上。	
步驟 8　违反文件类型过滤警告讯息 当使用者违反文件类型过滤时，将如右图在实时通讯窗口内出现警告讯息。	

14.3.5 实时通讯安全防护

14.3.5.1 防毒（Anti-Virus）

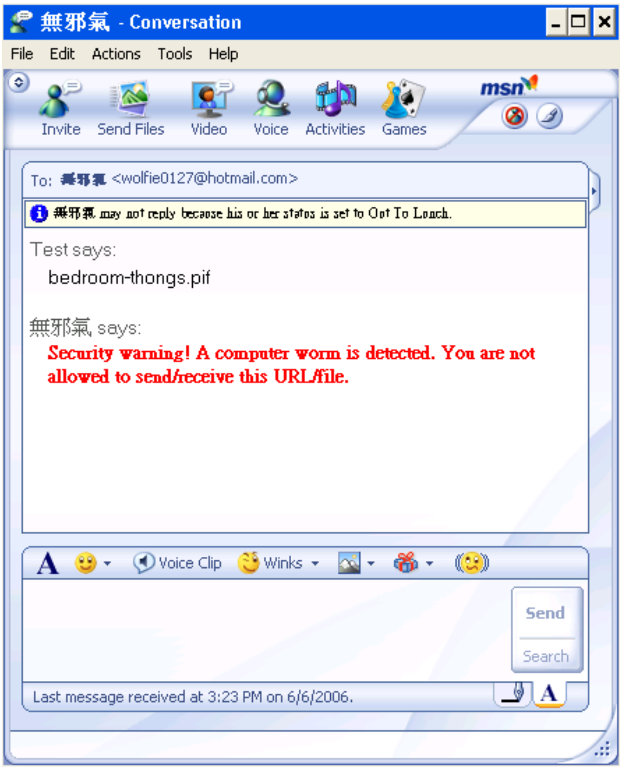
步驟 1 启用 ClamAV 防毒 勾选 **Enable ClamAV Anti-Virus**，然后选择您希望 InstantScan 扫描的最大档案大小。例如 500K，当传送的档案大小是 500K 以下才扫毒，超过 500K的档案一律放行。	**Functions > Management > IM Manager > IM Security > Anti-Virus** 
步驟 2 上传配置文件 选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。	
步驟 3 传送/接收的档案含有病毒的警告讯息 当用户传送/接收的档案含有病毒时，在您或聊天对象接收档案后，系统将会在实时通讯窗口内传送警告讯息告知 InstantScan 内部的用户。	

14.3.5.2 防蠕虫（Anti-Worm）

步驟 1 启用第七层防蠕虫 勾选 **Enable L7 Anti-Worm**。	**Functions > Management > IM Manager > IM Security > Anti-Worm** 
步驟 2 上传配置文件 选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。	

步驟 3 传送/接收的URL/档案含有病毒的警告讯息

当用户传送/接收的URL/档案含有计算机蠕虫时，系统将会在实时通讯窗口内传送警告讯息告知 InstantScan 内部的用户。

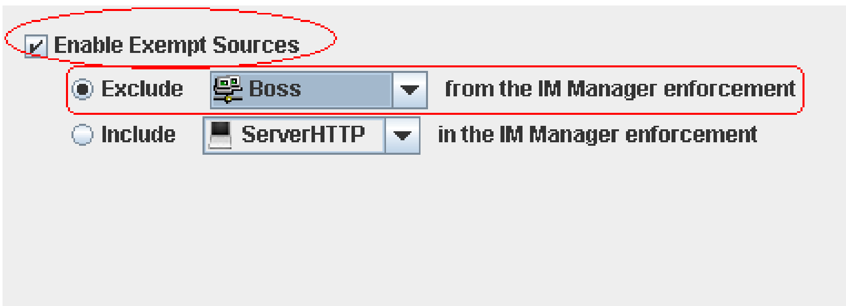


14.3.6 除外来源端设定

步驟 1 启用除外来源端

勾选 **Enable Exempt Sources**，然后选择 **Exclude Boss from the IM Manager enforcement**。在上面的章节我们已提过 Boss（包含 CEO 与 CTO）有完整的权限存取因特网，所以将其列入除外来源，避开实时通讯管理员的控管。

Functions > Management > IM Manager > Exempt Source



步驟 2 上传配置文件

选择 **Upload Configuration** 或点击图示 将配置文件上传到装置上。

字段	说明	范围 / 格式	范例
Enable Exempt Sources	启用除外来源功能。	启用 / 不启用	启用
Exclude ____ from IM Manager enforcement	所列举的 IP 地址除外，其余的计算机皆强制执行实时通讯管理政策。	所有 Object 地址/群组列表	Boss
Include ___ in IM Manager enforcement	实时通讯管理政策只适用于所列举的计算机。	所有 Object 地址/群组列表	--

表格 14-1 除外来源端字段解释

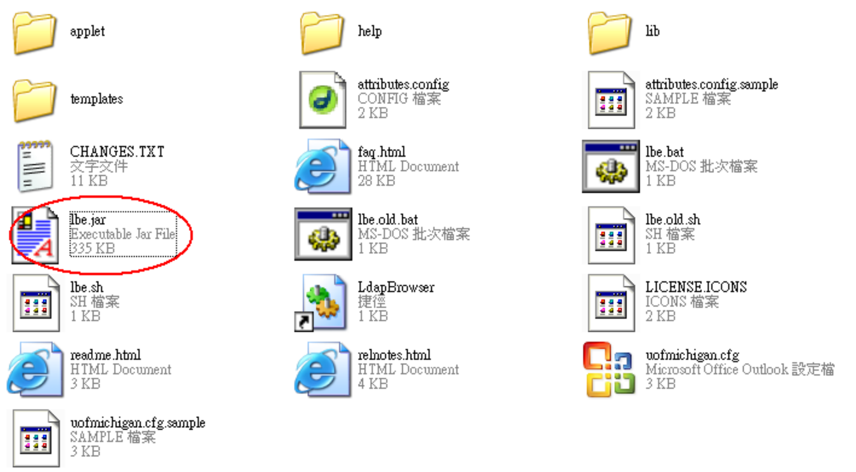
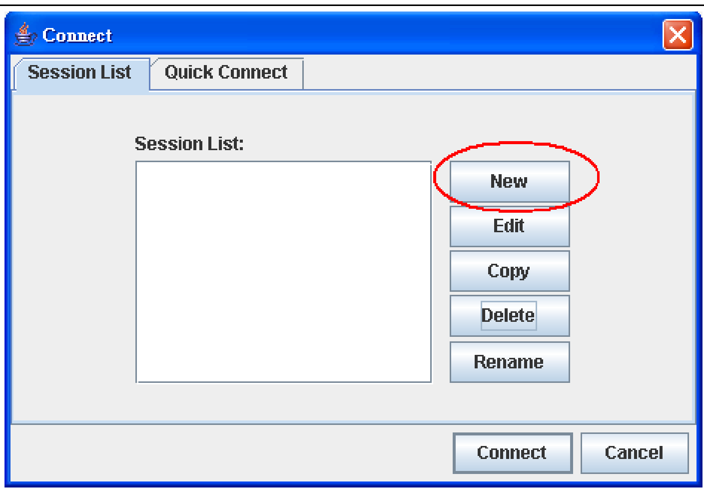
第15章
LDAP (ActiveDirctory) Import 设定范例

LDAP 代表 Lightweight Directory Access Protocol（轻量目录存取协议）。在 LDAP 的协议之中，很像硬盘目录结构或倒过来的树状结构。LDAP 的根就是全世界，第一级是属于国别（countries）性质的层级，之后可能会有公司（organization）的层级，接着是部门（organizationalUnit），再来为个人。而就像个人档案，每个人都会有所谓的显名（distinguished name，简称 dn），dn 可能类似 cn=John Smith,ou=Accounts,dc=myCompany,dc=tw。

针对 LDAP Import 这个功能，因其本身的复杂性，所以有许多使用者可能不甚了解如何设定。在此，我们提供详尽的设定范例，希望提供用户设定时的参考。

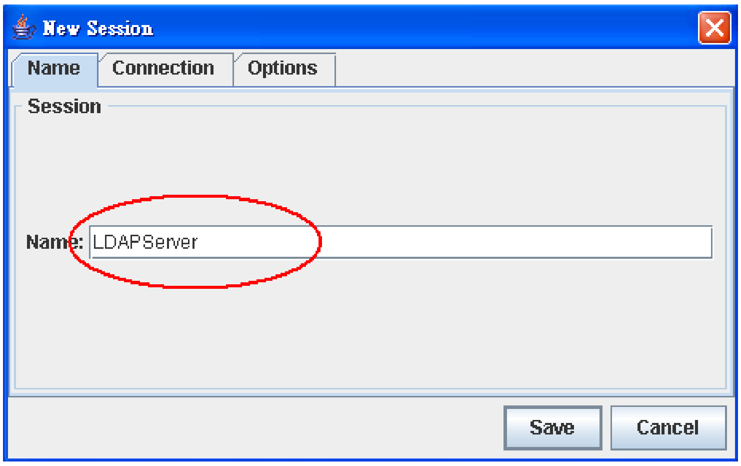
在使用 LDAP Import 这个功能之前，要先确认您现在用来操作用户接口的计算机是否可以透过 LDAP 这个 Protocol，联机到贵公司的 LDAP 服务器（例如：ActiveDirectory、OpenLDAP 等）。建议您先用一套 LDAP Browser 的软件来测试是否可以联机到 LDAP 服务器上，您可以在 http://www-unix.mcs.anl.gov/~gawor/ldap/ 这里找到这套软件以及更多 LDAP 相关信息。以下的范例为我们在上列网站上下载 Browser282b2.zip，解压缩后执行。

15.1 设定 LDAP Browser 软件

步驟 1 开启 LDAP Browser 软件 将鼠标移到 lbe.jar 档案上点两下。	
步驟 2 启用 LDAP Browser 软件 启动 LDAP Browser 的软件后，您可以看到如右图的画面，点击 New 建立新的联机（Session）。	

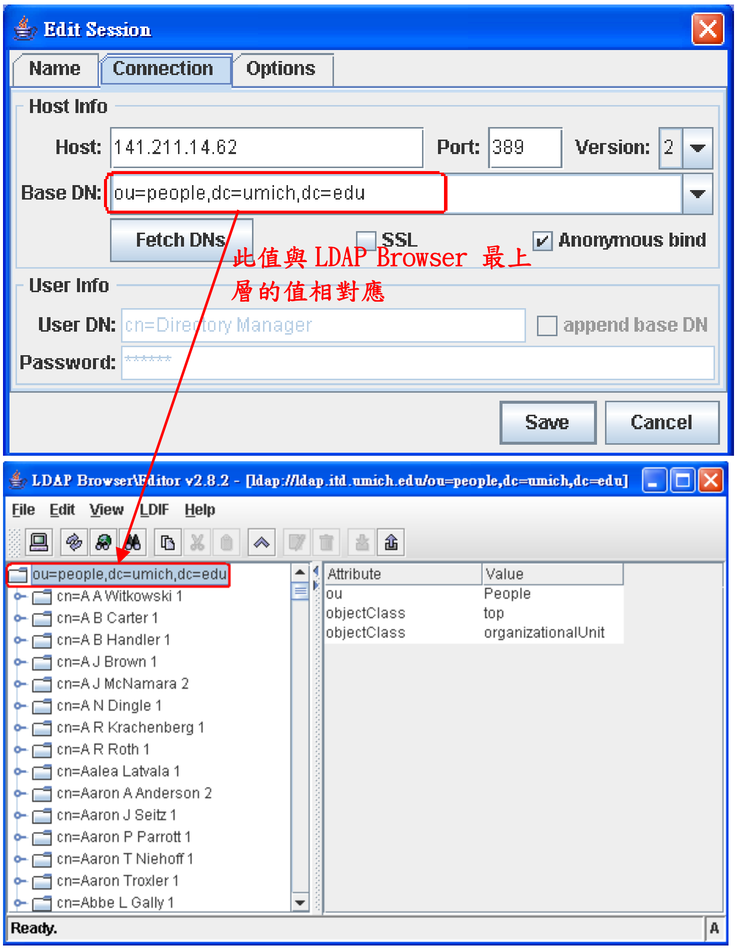
步驟 3 输入联机的名称

输入此联机的名称。



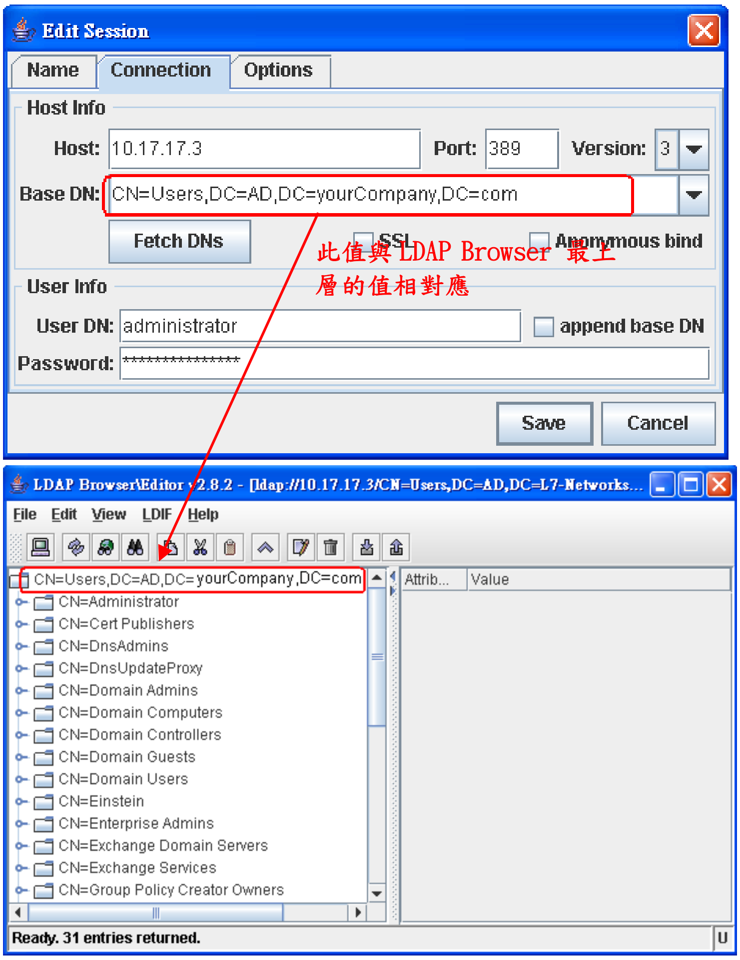
步驟 4 a 设定 LDAP 服务器联机参数 – OpenLDAP

输入 LDAP 服务器的 IP 地址或网址、端口与您在服务器上所设定的 Base DN。如果不确定 Base DN 为何，可以尝试用 Fetch DNs 来自动取得 Base DN。请注意，当您使用 Fetch DNs 时，所撷取到的 Base DN 为最上层的 Base DN。为了确保 LDAP Import 时数据的正确性，请务必确认用户数据所存放的 Base DN 为何。一般而言，OpenLDAP 用户数据会储存在ou=People 的路径目录下。



步骤 4b 设定 LDAP 服务器联机参数 – ActiveDirectory

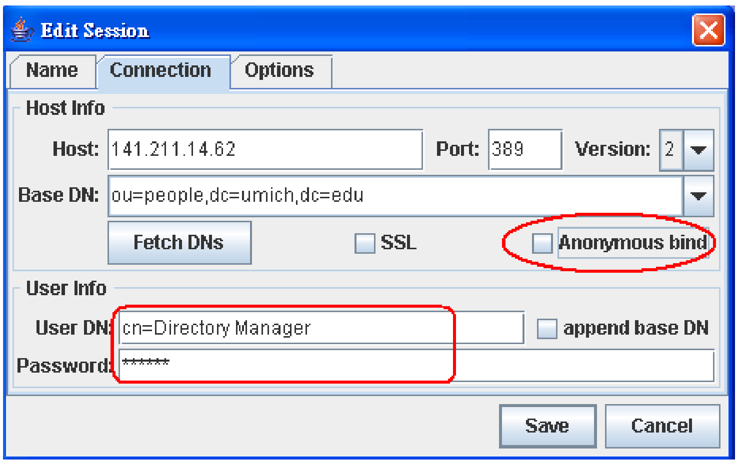
输入 LDAP 服务器的 IP 地址或网址、端口与您在服务器上所设定的 Base DN。如果不确定 Base DN 为何，可以尝试用 Fetch DNs 来自动取得 Base DN。请注意，当您使用 Fetch DNs 时，所撷取到的 Base DN 为最上层的 Base DN。为了确保 LDAP Import 时数据的正确性，请务必确认用户数据所存放的 Base DN 为何。一般而言，ActiveDirectory 用户数据会储存在 cn=Users（ActiveDirectory） 的路径目录下。

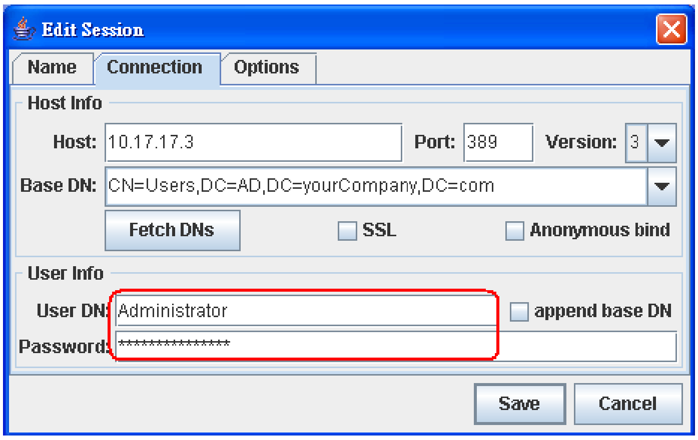
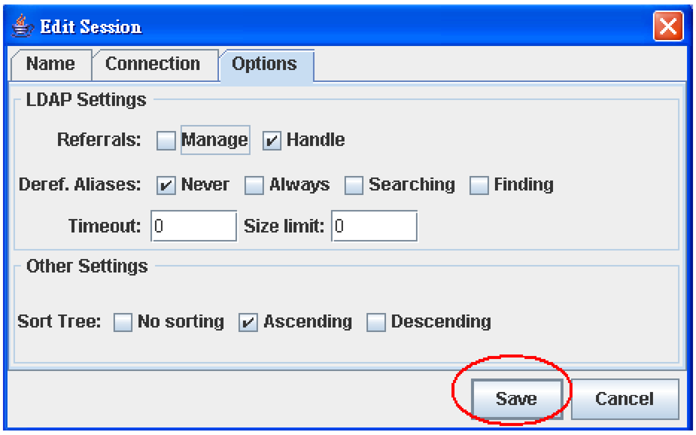
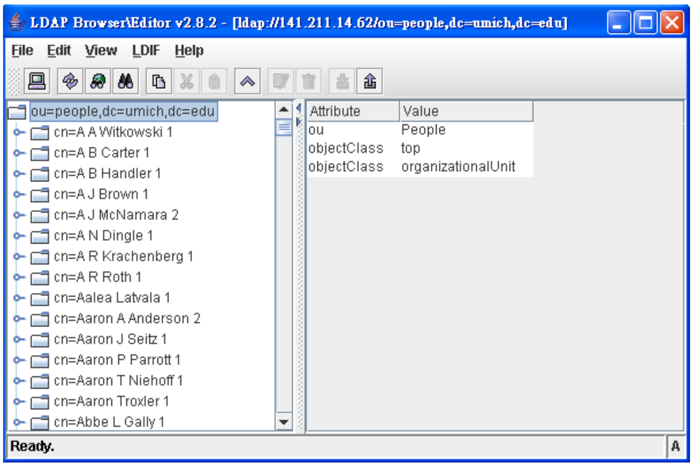


步驟 5 a 取消匿名绑定设定 - OpenLDAP

取消勾选匿名绑定（anonymous bind），然后在 User DN 那边输入管理者的账号与密码。

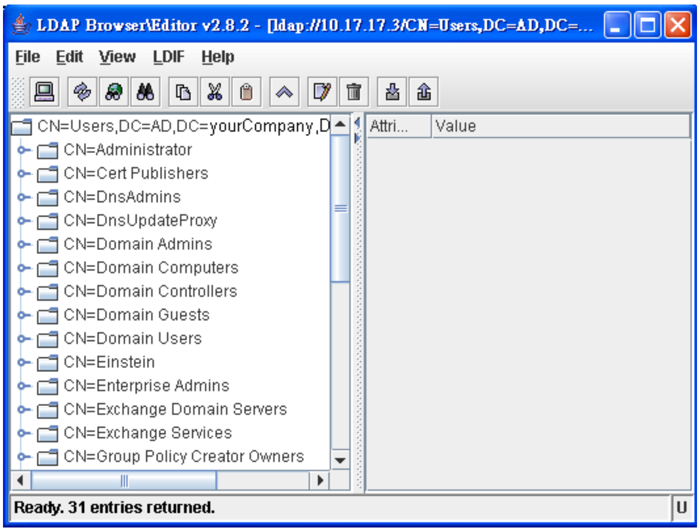
注意: 在Open LDAP中您所输入的 User DN必须为 cn=[yourAccount]，例如 cn=Directory Manager。



步骤 5b 取消匿名绑定设定 - ActiveDirectory 取消勾选匿名绑定（anonymous bind），然后在 User DN 那边输入管理者的账号与密码。	
步骤 6 进阶设定 在 Options 这边有些其他相关的设定，可以视你的需求去调整。一般而言不需要更动。	
步骤 7 a 测试联机状况 - OpenLDAP 最后使用这个已经设定好的联机，如果可以成功看到服务器上所储存的资料，则表示联机正常，如果联机不正常的话，请参考**错误！找不到参照来源。**试着排解问题。	

步骤 7b 测试联机状况 - ActiveDirectory

最后使用这个已经设定好的联机，如果可以成功看到服务器上所储存的资料，则表示联机正常，如果联机不正常的话，请参考**错误！找不到参照来源。错误！找不到参照来源。**试着解决问题。



15.2 设定 LDAP Import – 基本设定

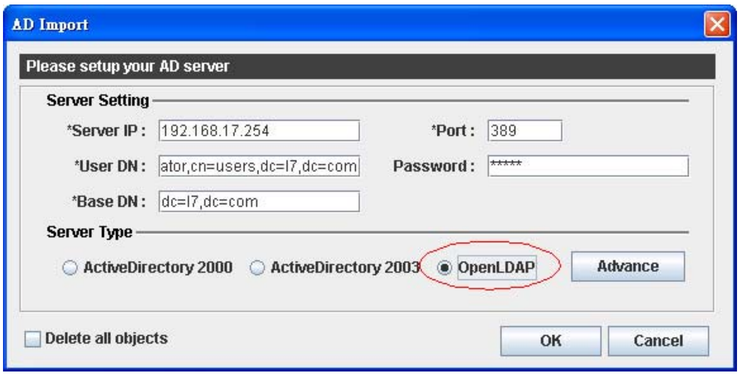
步驟 1 设定 LDAP Import 参数

设定服务器的 IP、端口，以及管理者的账号密码。并且设定服务器上的 Base DN。

步驟 2 选择 LDAP 服务器类型

选择您的LDAP Server类型，选择正确的Server类型，会帮您做好预设筛选用户与群组信息的方式。如果您需要自行调整LDAP内容参数，请参考进阶设定中的说明。

A: OpenLDAP



B: ActiveDirectory



15.3 设定 LDAP Import – 进阶设定

步驟 1 设定过滤器

设定使用者的过滤器（filter），指定的过滤器会把满足条件的数据视为有效的用户数据，否则该笔数据将会被略过，关于过滤的设定方式请参照搜寻过滤条件的字符串表示法，定义于 RFC 2254（http://www.ietf.org/rfc/rfc2254.txt）中。

步驟 2 名称与描述的进阶设定

设定汇入时每笔用户数据中，指定要当做使用者名称（name）、描述（description）以及群组（Group）的字段。

步驟 3 选择汇入方式

设定群组所在的Base DN，指定的目录与其子目录，即为汇入群组信息的范围。

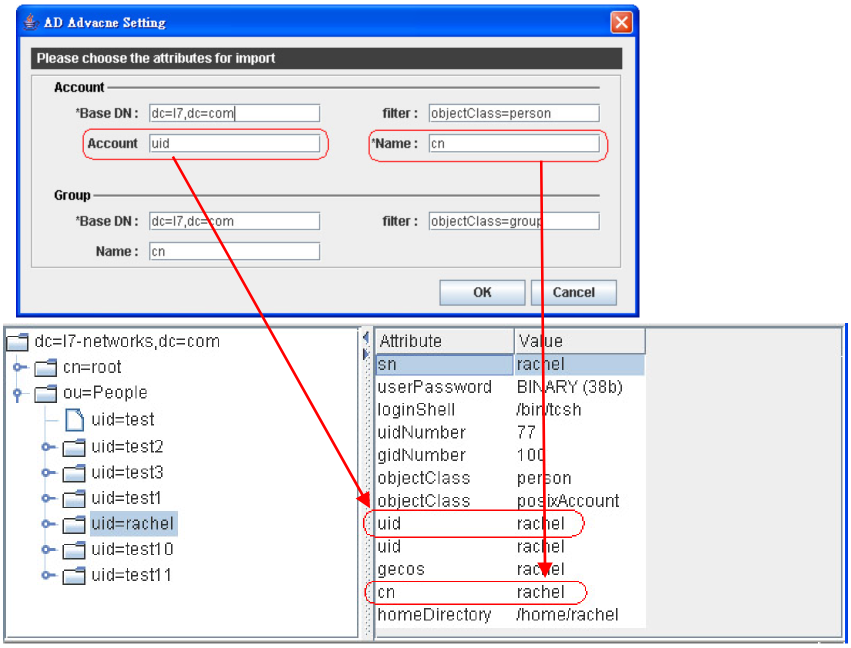
步驟 4 汇入字段设定

设定群组参照的字段，一般在用户的信息中，群组字段的内容不是简单的组名，而是参照用的数字或者字符串，所以在群组信息中，通常也会有一个字段做为参照用，只要比对用户信息中的群组字段与群组信息中的参照域值是否相同，就可以判断此一使用者是否属于此一群组。

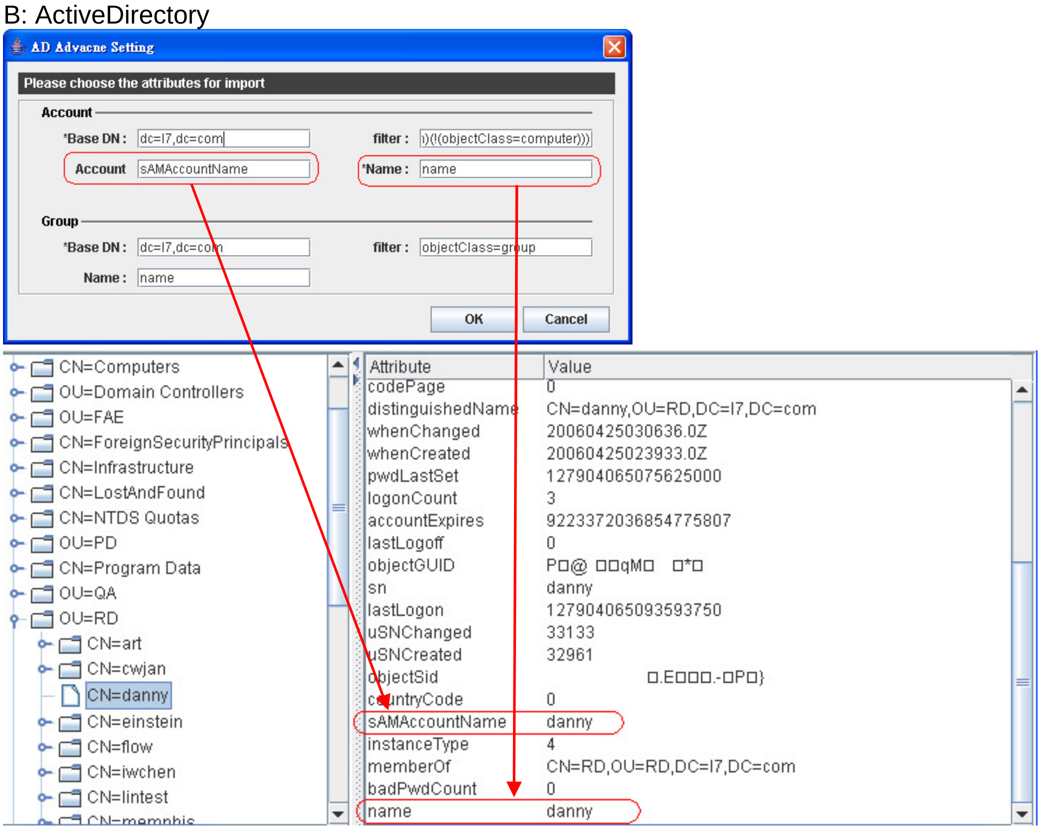
步驟 5 数据汇入

设定汇入每笔群组数据中，指定要当组名（name）、描述（description）的字段。

A: OpenLDAP



B: ActiveDirectory



15.4 LDAP 汇入疑难解答

问题一：为何我无法连到我的 LDAP 服务器？

答：首先要先确认服务器的 IP 与端口是否正确。如果没有错误的话，可以用 telnet <ip> <port>的方式，看看是否能正常连接。在操作 UI 的计算机与 LDAP 服务器之间是否有防火墙阻挡？LDAP 服务器设定是否有开放权限，让外部的计算机存取（access）数据？（关于 LDAP 服务器要怎么设定存取权限，请洽询你的 LDAP 服务器软件供货商。

问题二：为何汇入成功，却没有新增任何用户数据？

答：这可能是因为你所指定要汇入信息的位置错误，或者过滤器的条件设定有误，以致于没有任何信息符合条件。

问题三：为何我所汇入的使用者数量比我存在 LDAP 服务器上的还要少？

答：因为多数 LDAP 服务器会设定一次查询（query）中，能响应结果（result）的数量上限，如果希望能正常汇入所有用户的数据，必须要修改你所使用的 LDAP 服务器的参数。请参照 http://www.ldapbrowser.com/forum/viewtopic.php?t=14 的讨论，或者请洽询你的 LDAP 服务器软件供货商。

第16章
封装管理员

本章节介绍 InstantScan 的封装管理功能与其设定。

16.1 需求

1. 当管理 MSN 与 Yahoo 实时软件入下联机时，不须要更改任何的防火墙与使用者端的设定

16.2 方法

1. 在 Functions > Management > Enapsulation Manager 页面上开始封装管理员即可。

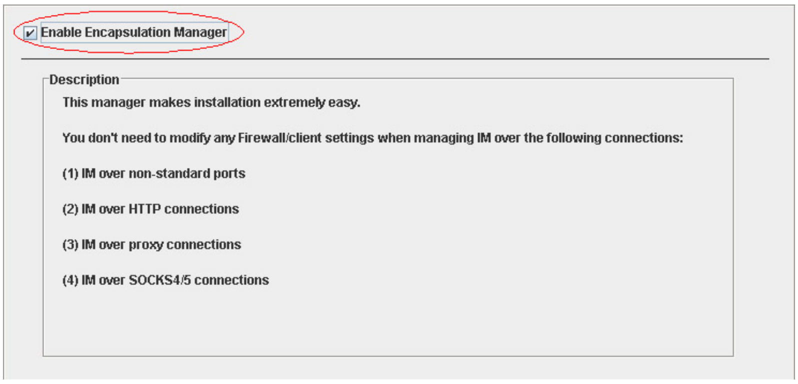
16.3 步骤

16.3.1 启动封装管理员

步骤 1 开启封装管理员

勾选 Enable Encapsulation Manager。

Functions > Managements > Enapsulation



步骤 2 上传配置文件

选择 **Upload Configuration** 或点击图示  将配置文件上传到装置上。

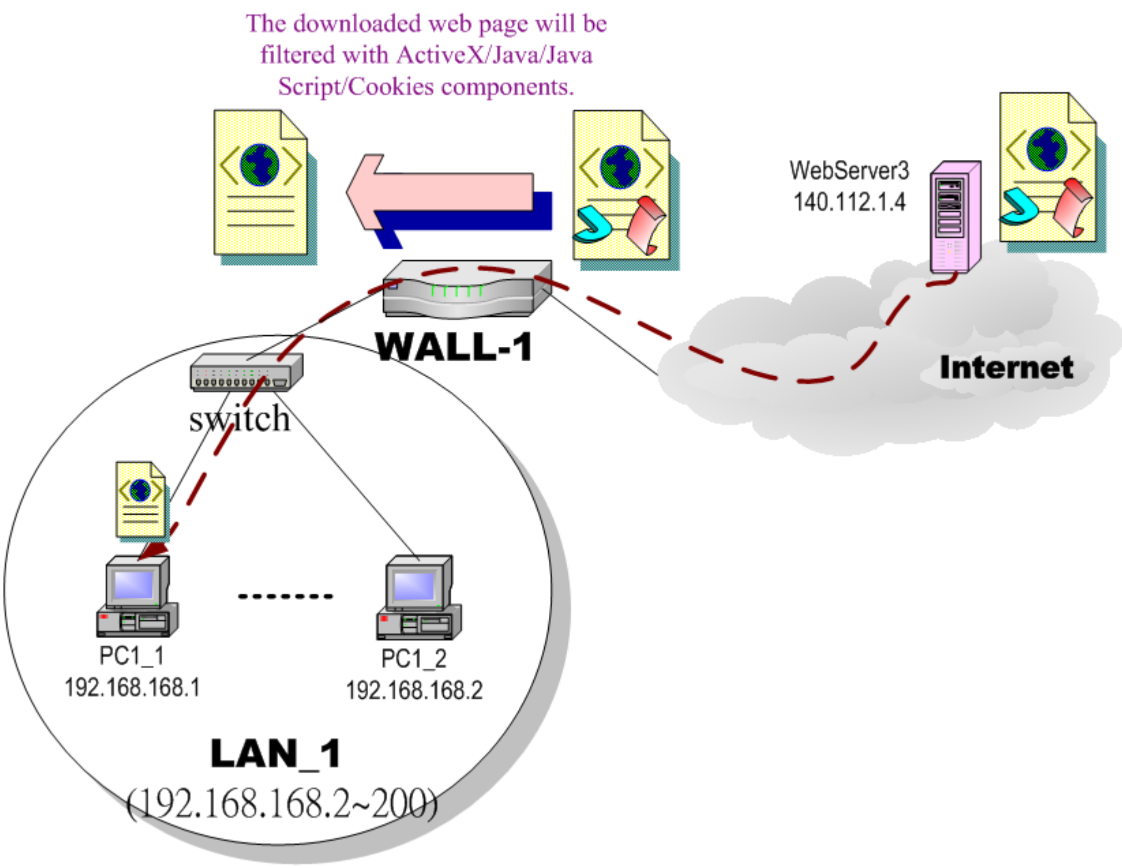
第8部

网页管理员

第17章
网页管理员

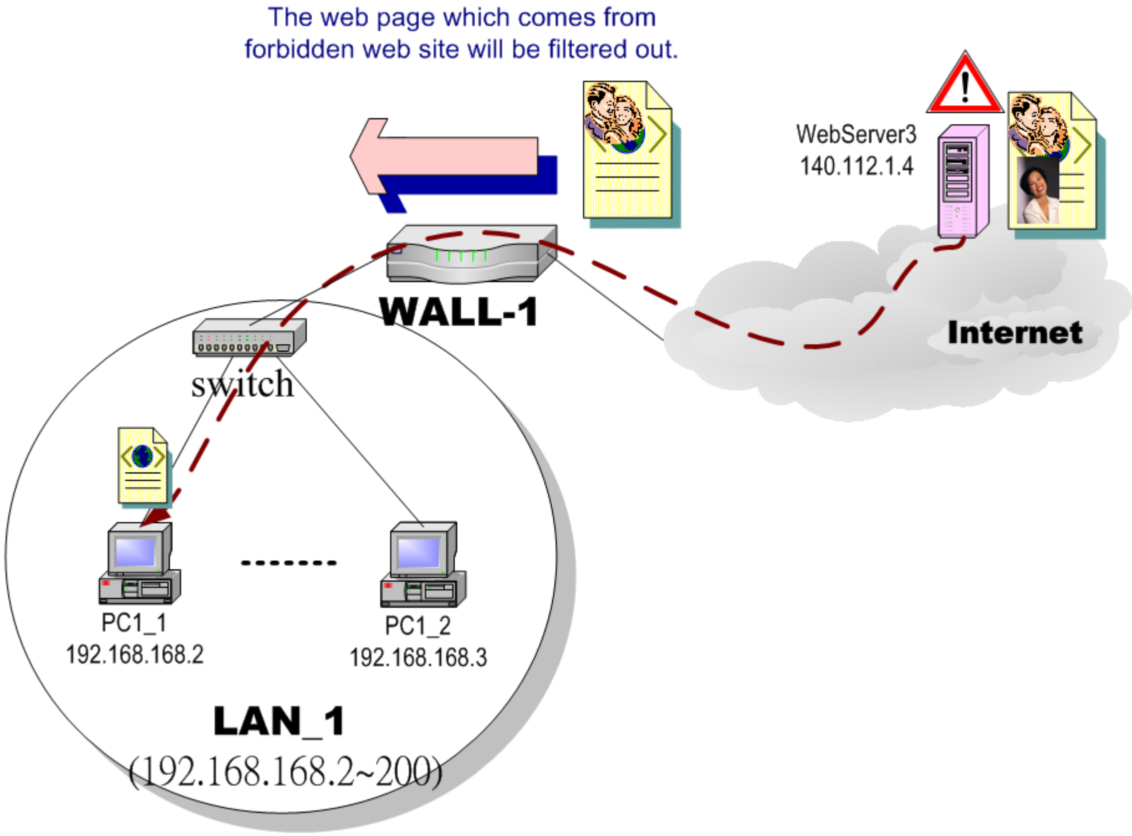
本章节介绍IntantScan 的网页管理功能与其设定。

17.1 需求



图表 17-1 透过网页过滤防止员工浏览被禁止的网站

1. 如图表 17-1 所示，PC1_1 正在浏览 WebServer3 的网页。网页的内容包含 cookies、Java applets、Java scripts 或者 ActiveX 对象等，这些内容也许包含恶意软件伺机窃取用户数据。所以，您希望能够禁止 PC1_1 下载这些禁止浏览的组件。



图表 17-2 透过网页过滤禁止员工浏览 WebServer3 的网页

2. 如图表 17-2 所示，PC1_1 在上班时间浏览禁止浏览 WebServer3 的网页。这些网页内容也许包含股票市场信息、暴力或色情，且会浪费公司因特网的带宽，降低员工生产力。所以，您希望透过设定 InstantScan 就可以拦阻 PC1_1 浏览这些类型的网站。

17.2 目的

1. 移除网页内含的 cookies、Java applet、ActiveX 对象等。
2. 防止员工连上禁止浏览的网站。

17.3 方法

1. 设定要过滤的网页组件，例如 cookies 或 Java applets。
2. 设定网页过滤。当浏览网页时，InstantScan 会根据设定的规则检查网域、网址或关键词来判断是否放行网页流量。

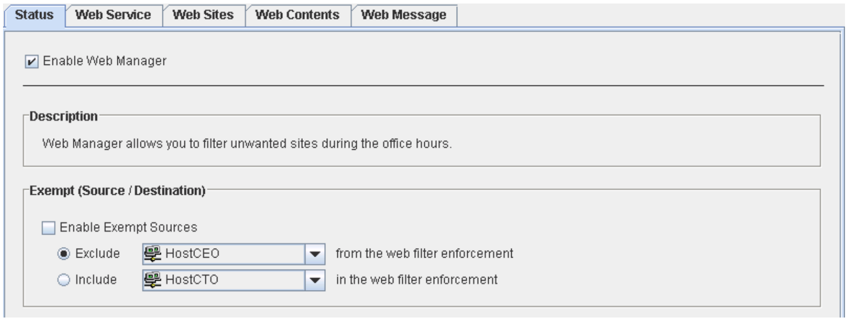
17.4 步骤

步驟 1 启用网页过滤

勾选 **Enable Web Filter**。

请注意，当您套用网页过滤时，系统将自动勾选过滤所有流经标准 HTTP（80埠号）的网页流量。若想要将某些人除外，可勾选**Enable Exempt Sources**，其中Exclude是除外，Inlcude是只对选定的人进行Web过滤。

Content Manager > Web Manager > Status

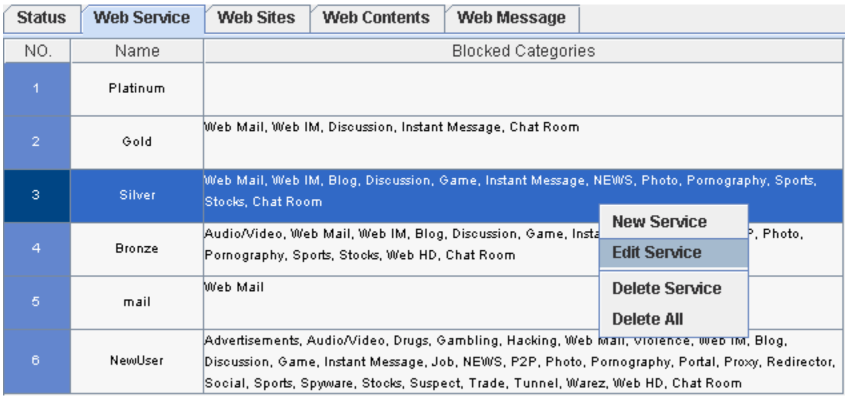


步驟 2 编辑Web Service

决定Web Service的各个权限等级。

你可以新增Web Service，或者编辑现有Web Serivce。

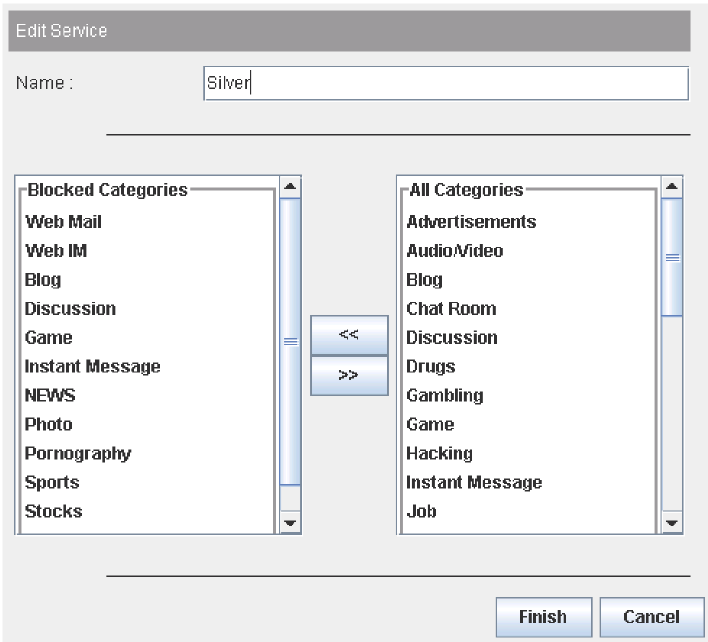
Content Manager > Web Manager > Web Service



步驟 3 编辑Silver Web Service

将您想要阻挡的Web database网站种类，加到Silver等级的Web Service。若用户被指定为此Service者，连到这几种网页时，就会被阻挡。

Content Manager > Web Manager > Web Service > Edit Service

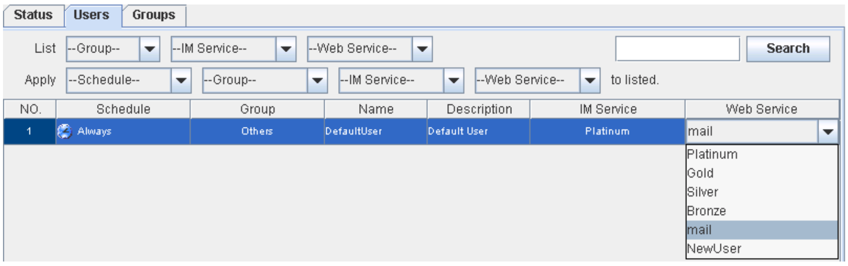


步骤 4 于用户控制台加入用户

你可以从AD Import进来用户数据，然后让用户登入时自动让系统得知AD登入，并对其后的Web Service作相对应的过滤。

系统内建DefaultUser，任何没有比对身份到的Web流量，都会给予设定的Web Service。

Functions > Console > User Console

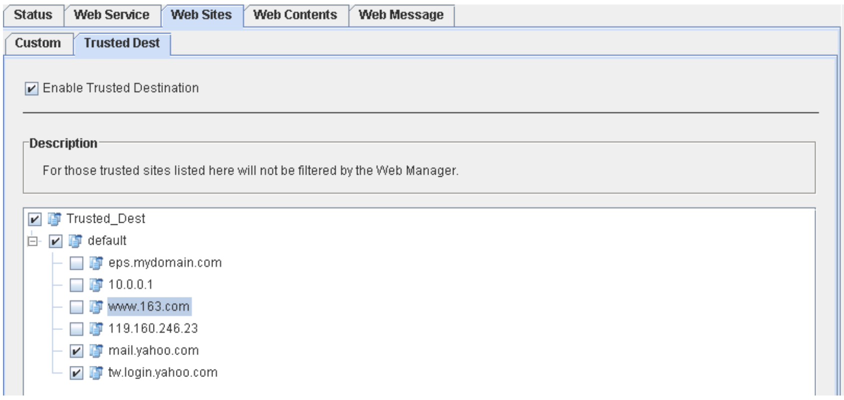


步骤 5 订定信任的网域

勾选 Enable Trusted Domain。然后新增信任的网域群组与网域名称。

请输入信任的网域名称。注意，如果您所输入的网域名称无法被 DNS 服务器辨识，这笔网域名称将会被忽略。再则是，如果您启用太多的网域名称，在开始网页过滤时将需要较长的时间来作名称辨识。

Management > Web Manager > Exclude > Trusted Dest



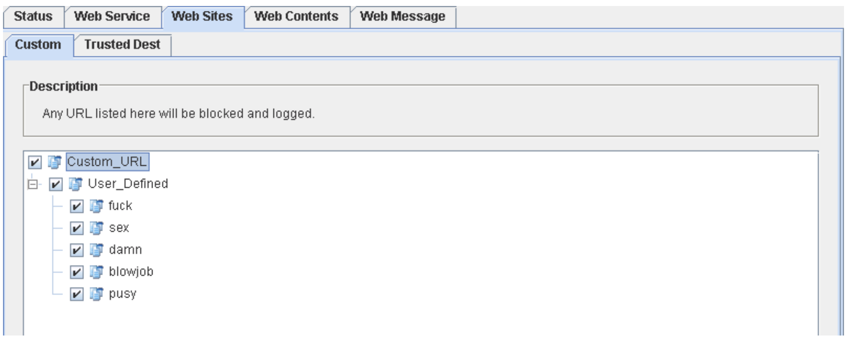
字段	说明	范围 / 格式	范例
Enable Exempt Sources	启用用除外来源端。	启用 / 不启用	启用
Exclude ____ from the web filter enforcement	所列举的 IP 地址除外，其余的计算机皆强制执行网页过滤。也就是说当您选择 Boss 时，除了 CEO 与 CTO 外的 IP 都需要执行网页过滤。	启用 / 不启用	启用 / Boss
Include ___ in the web filter enforcement	网页过滤只适用于所列举的计算机。	启用 / 不启用	不启用

表格 17-1 除外来源端字段说明

步骤 6 客制化 URL 关键词拦阻

勾选 **Custom_URL**，拦阻任何包含关键词列表之 URL 地址。InstantScan 已默认一些常用的关键词，如不敷需求您可以在屏幕上右键单击新增/修改/删除关键词群组/关键词。

Functions > Management > Web Manager > Web Sites > Custom



字段	说明	范围 / 格式	范例
URL Keywords	如果您要浏览的 URL 网址出现所输入的关键词，当您利用因特网连上此网址后，此 URL 的内容将会被 InstantScan 拦阻。	文字字符串	Adv/advertise/adsrv/banner/splash

表格 17-2 URL 关键词过滤

步驟 7 网页对象特征过滤

勾选 Enable Object Blocking。然后勾选要利用特征过滤的网页对象。当您启用此功能后，透过 PC1_1 浏览网页可能还可以看到这些对象。这可能是因为网页暂存（cache）所致。请清除所有网页浏览器内的网页暂存记忆，关闭浏览器。重新开启浏览器，然后重连网页即可。

Functions > Management > Web Manager > Web Contents > Object



字段	说明	范例
启用对象特征拦阻	选择以下的网页组件以作为网页之特征过滤。	启用
ActiveX	过滤包含 ActiveX 的网页。	启用
Java	过滤包含 Java 的网页。	启用
Cookies	过滤包含 Cookies 的网页。	启用

表格 17-3 网页特征过滤

字段	说明	范围 / 格式	范例
Enable Keyword Blocking	启用网页内容关键词拦阻。	启用 / 不启用	启用
Stop transferring the web page when the same keyword appears for __ times.	当勾选关键词拦阻，如果您要开启的网页中含有本页所列举的关键词，此网页将会被拦阻而无法正常显示。"限关键词每出现 __ 次" 意味着只要关键词出现等于或大于所输入的数字时，拦阻要开启的网页。例如，只要关键词出现 5 次，拦阻该网页。	启用 / 不启用 数字	启用 5 次
Keywords	输入您想拦阻的关键词。	文字字符串	adv advertise adsrv banner splash

表格 17-4 网页关键词过滤

第9部

报表系统

第18章
报表系统简介

本章介绍 InstantScan 报表系统。

18.1 InstantScan 报表系统

InstantScan 提供客户随选即用人性化的用户接口，除了易于设定的管理系统外，更提供用户简洁易懂的报表系统。让用户可以依据需求定义报表搜寻方式、查询各式各样的排行榜数据、更可依功能面、政策面与个人面作特殊的搜寻与排行。除此之外，更有事件记录的数据可供用户查询。

18.2 报表设计原则

18.2.1 报表类别

目前 InstantScan 依功能列分成五种报表：

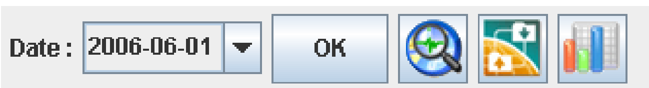
1. 应用层防火墙报表：可检视与查询所有应用层防火墙通讯协议的排行榜与事件记录。
2. 实时通讯管理员报表：可检视与查询所有实时通讯行为的排行榜与事件记录。
3. 网页管理员报表：可检视与查询所有网页流量的图形报表与事件记录。
4. 流量管理员报表：可检视与查询每日、每周、每月、每季与每年的流量排行榜与事件记录。
5. 系统管理员报表：可检视与查询所有系统的操作信息。详见**錯誤! 找不到參照來源。**系统纪录的说明。

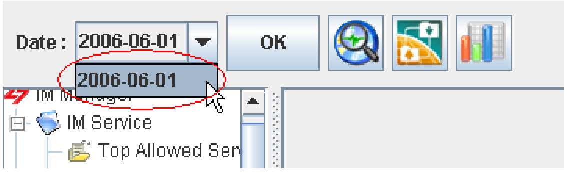
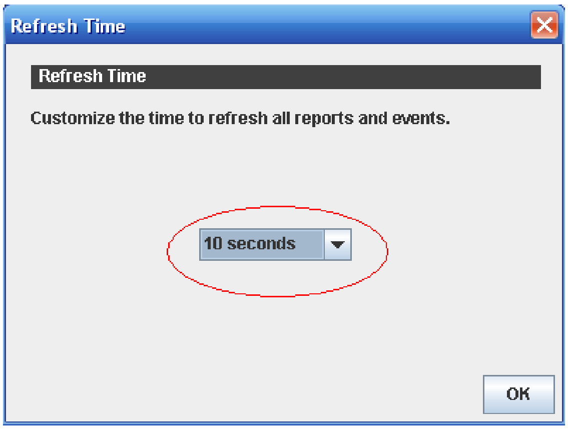
所有报表，除了系统管理员报表外，皆依其性质分成四个类别：

1. 功能面（Funcational View）：依功能作用排行。
2. 政策面（Policy View）：依使用者所制定的政策排行，也可以说是管理面的报表。
3. 个人面（Personal View）：依个别使用的状况排行，也可以说是个人化的报表。
4. 事件面（Event View）：所有行为动作的事件记录。

18.2.2 搜寻工具

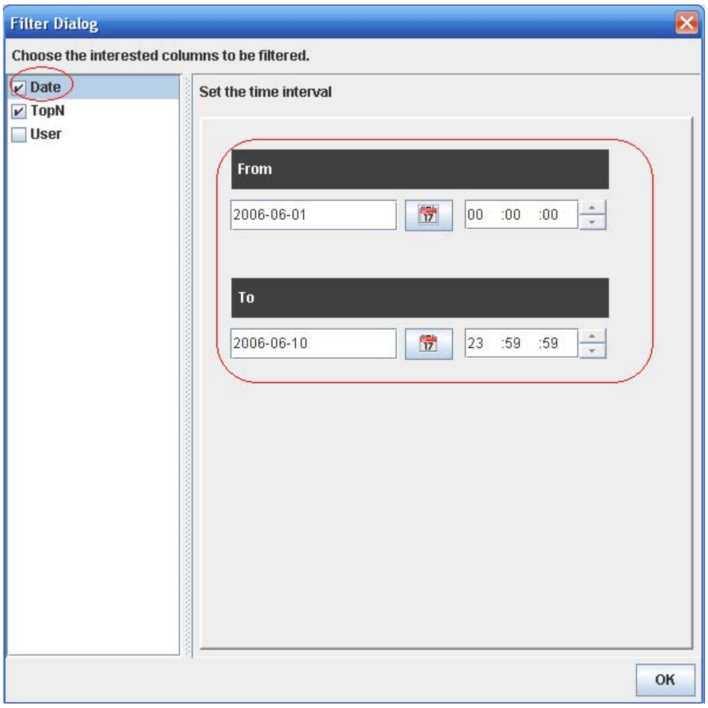
为了加速用户在寻找特定事件记录或报表的速度，InstantScan 搜寻工具栏可以让您依日期或特定的关键词搜寻你要的信息。



步驟 1 搜寻期间设定 报表系统上所显示的日期期间为您在安装管理服务器时所选择的数据分割期间。可分成 1) 每周 2) 每月 3) 每季，三种期间。如右图所示，分割期间为每个月。所以日期显示会以每个月的第一天为主，例如 2006-06-01。同理类推。 **注意，为了确保数据搜寻的速度与保留数据的完整性，在数据分割后，当您选择每周/每月/每季后，您无法跨周/月/季搜寻。**	
步驟 2 重新整理报表与事件记录时间设定 点击图示 设定重新整理报表与事件记录的时间。	
步驟 3 选择重新整理时间 选择 10 seconds，然后点击 **OK** 完成设定。一旦您套用这个设定，往后每 10 秒钟系统会根据您所选择的时间重新整理报表与事件纪录的数据。	
步驟 4 进阶搜寻 点击图示 （进阶）。	

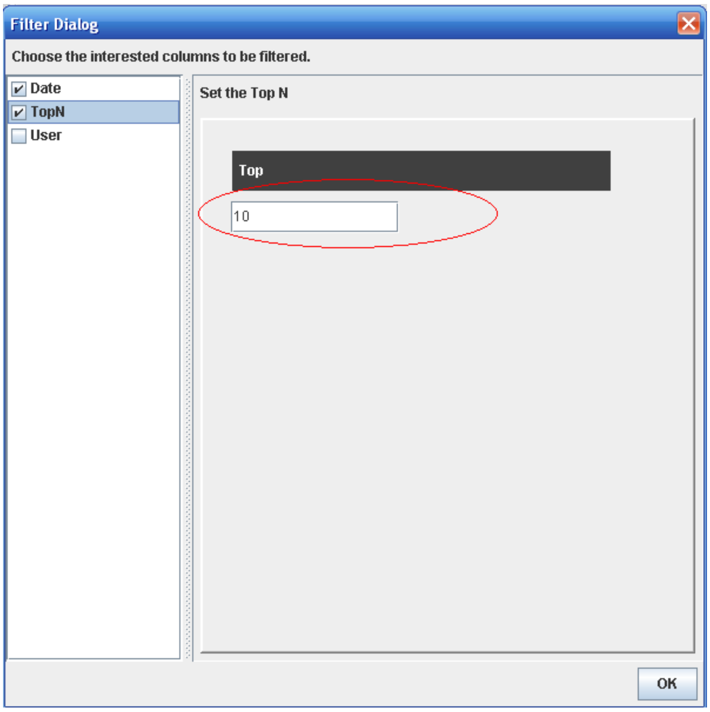
步驟 5 选择搜寻日期

勾选 Date。在此您可以缩小搜寻的范围。也就是说当您数据分割是以每月为主，您可以在当月内选择一个时间区段作数据搜寻的期间。请在时间间隔内选择搜寻的起始时间与结束时间。



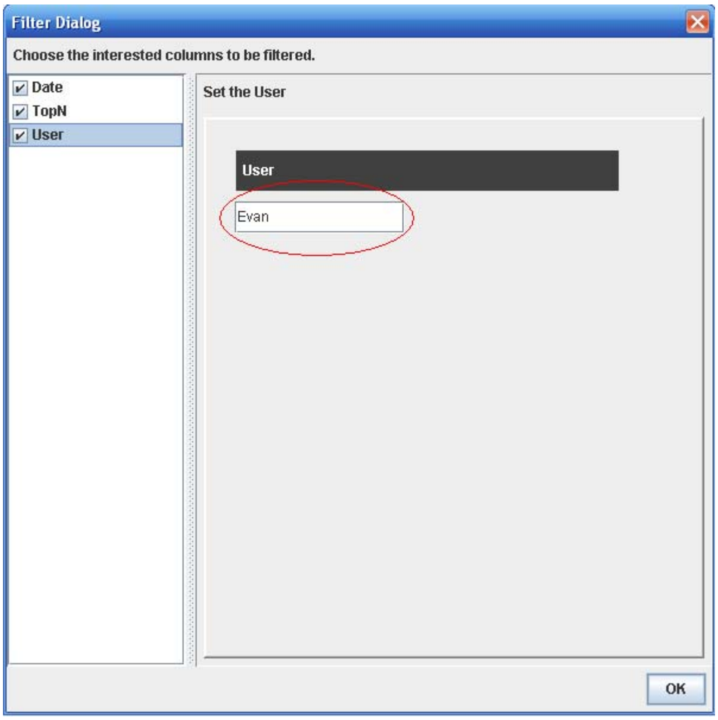
步驟 6 输入要浏览的排名数

勾选 TopN 默认上，系统显示的所有事件的排名列表，如果您只需要前 N 名排名列表，您可以在空格内输入您想要浏览的数目。



步驟 7 细部搜寻

如果您希望做更细部的搜寻，您可以特定的细部搜寻项目。例如：user、receiver、sender、application、action 等等，视您所选择的报表项目而定。



第19章
应用层防火墙报表

本章介绍应用层防火墙报表的应用。

19.1 需求

1. 有鉴于网络带宽的滥用频繁，管理人员希望获得哪些通讯协议被企图非法使用的统计数据。
2. 管理人员希望知道前 10 名使用 skype 被 InstantScan 拦阻的排行榜。
3. 管理人员希望知道使用者（IP：192.168.17.58）前 10 名被拦阻的通讯协议排名。
4. 管理人员希望将事件记录储存成 Excel 文件，可以依据自己的需求产生其他的报表格式。

19.2 方法

1. 到 Reports > Application Firewall > Funcational View > Top Blocked Protocol 检视图形报表。
2. 到 Reports > Application Firewall > Policy View > Top Blocked Users of Application，并于 Advanced 上勾选 Application 选择 skpye。
3. 到 Reports > Application Firewall > Personal View > Top Blocked Applications of User，并点击 Advanced 设定搜寻 source IP 192.168.17.58。
4. 到 Reports > Application Firewall > Event View，点击 Export，选择数据导出类型为 Excel。

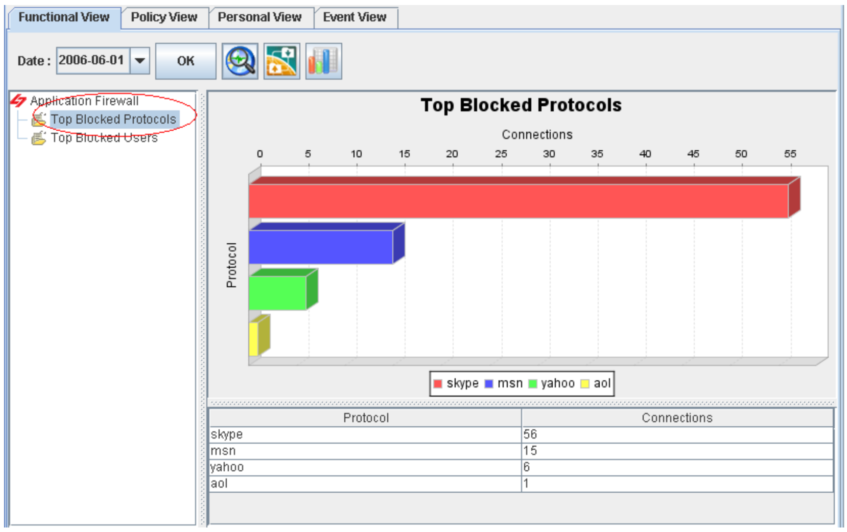
19.3 步骤

19.3.1 功能面报表浏览

步驟 1 点击被拦阻的通讯协议排行

点击 **Top Blocked Protocols**。

Reports > Application Firewall > Functional View > Top Blocked Protocols



报表项目	说明
Top Blocked Protocols	经常被拦阻的通讯协议排行。也就是企图非法闯关的通讯协议排行。
Top Blocked Users	经常被拦阻的使用者排行。也就是企图非法使用某些通讯协议的使用者排行。

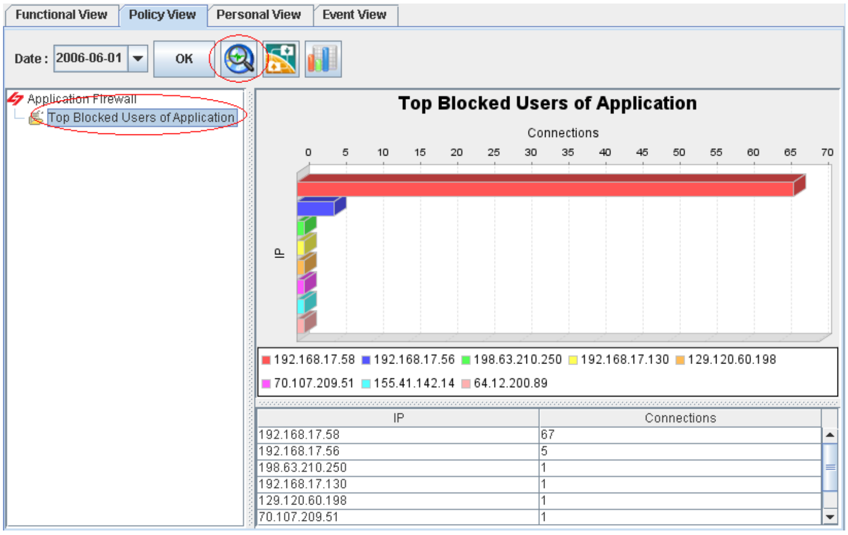
表格 19-1 应用层防火墙 - 功能面报表说明

19.3.2 政策面报表浏览

步骤 1 浏览因违法使用通讯协议而被拦阻的使用者排名

点击 **Top Blocked Users of Application**。然后点击图示  进阶设定。

Reports > Application Firewall > Policy View > Top Bloced Users of Application



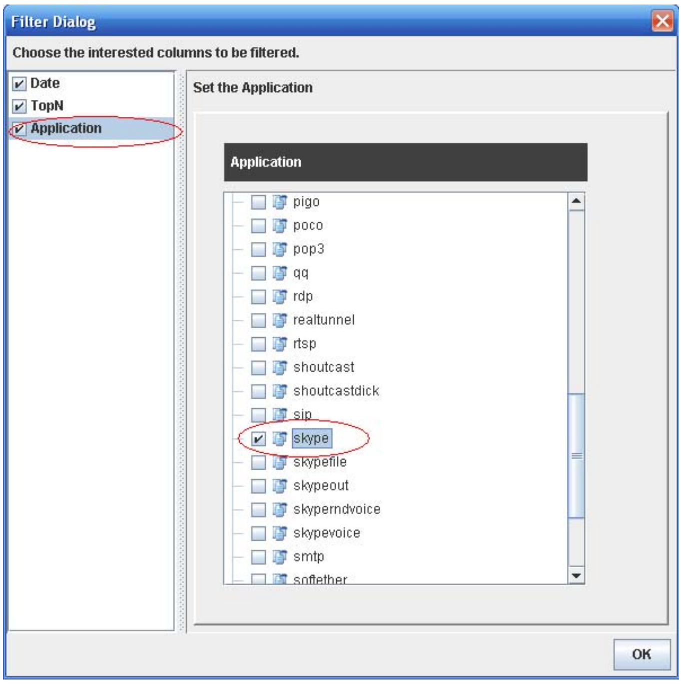
报表项目	说明
Top Blocked Users of Application	经常因违法使用通讯协议的使用者排行。

表格 19-2 政策面报表说明

步骤 2 进阶搜寻报表

勾选 Application，然后在 Application 列表上勾选 **Skype**。点击 **OK** 浏览结果。

Reports > Application Firewall > Policy View > Top Blocked Users of Application > Advanced



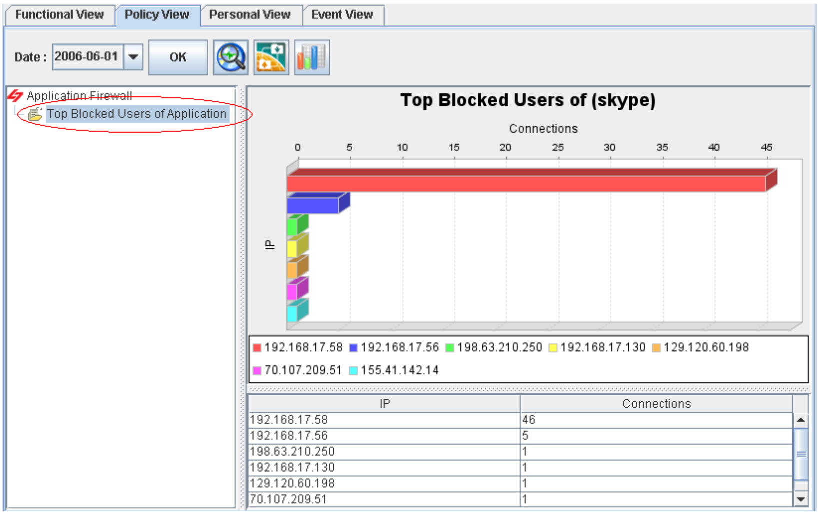
报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为当您在管理服务器所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Application	您希望浏览哪些使用者经常违法使用某些通讯协议的排行。可复选。	skype

表格 19-3 应用层防火墙 - 政策面报表进阶搜寻说明

步骤 3 浏览设定的结果

右图为因为企图非法使用 Skype 的使用者排名。

Reports > Application Firewall > Policy View > Top Blocked Users of Application

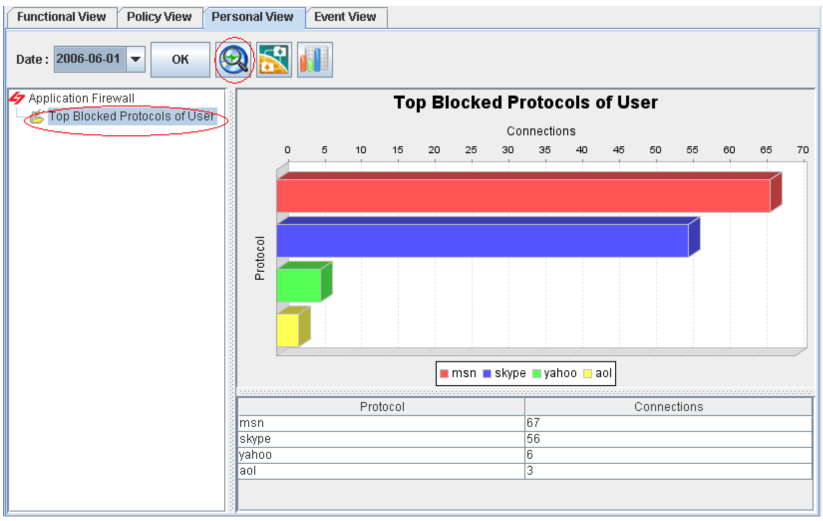


19.3.3 个人面报表浏览

步骤 1 浏览使用者所违法使用的通讯协议排行

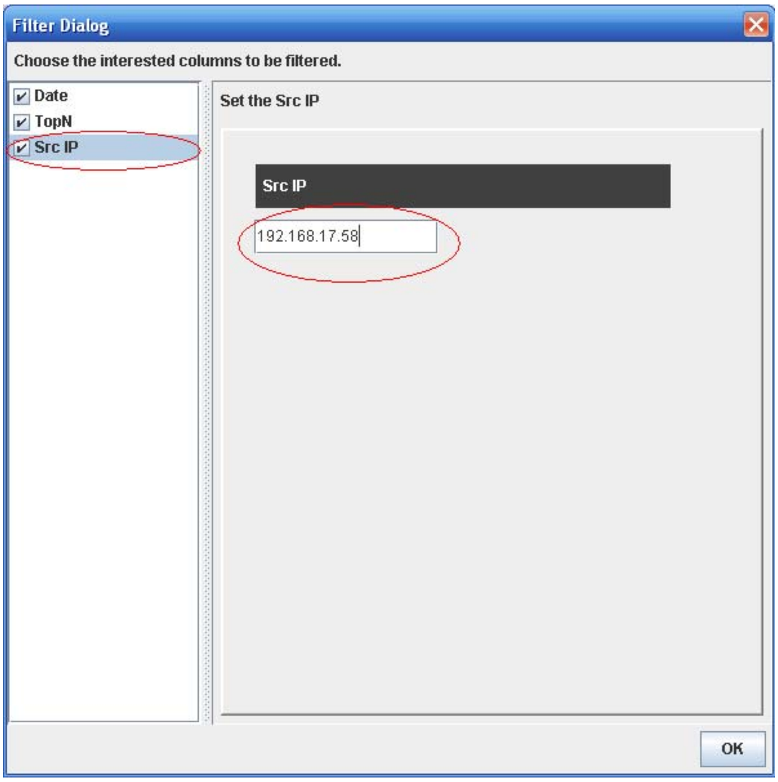
点击 **Top Blocked Protocols of Users**。然后点击图示  进阶设定。

Reports > Application Firewall > Personal View > Top Bloced Protocols



报表项目	说明
Top Blocked Protocols of User	特定的使用者所违法使用的通讯协议排行。

表格 19-4 应用层防火墙 - 个人面报表说明

步驟 2 进阶搜寻报表 勾选 Src IP，然后在 Src IP 字段上输入 **192.168.17.58**。点击 **OK** 浏览结果。	**Reports > Application Firewall > Personal View > Top Blocked Protocols of User > Advanced** 

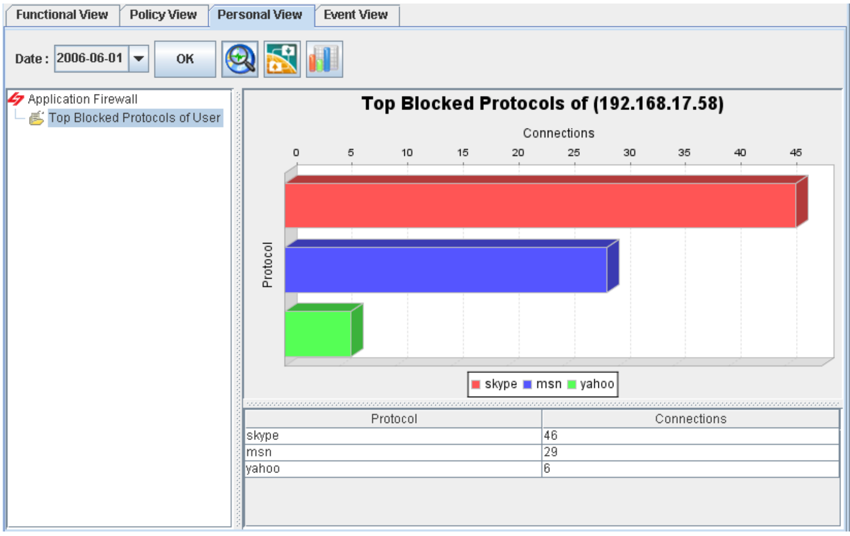
报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为您在管理服务器所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Src IP	您希望查询的使用者，其经常违法使用而被拦阻的通讯协议排行。	192.168.17.58

表格 19-5 应用层防火墙 - 个人面报表进阶搜寻说明

步驟 3 浏览搜寻结果

右图使用者 192.168.17.58 企图非法使用的通讯协议排行表。

Reports > Application Firewall > Personal View > Top Blocked Protocols of User

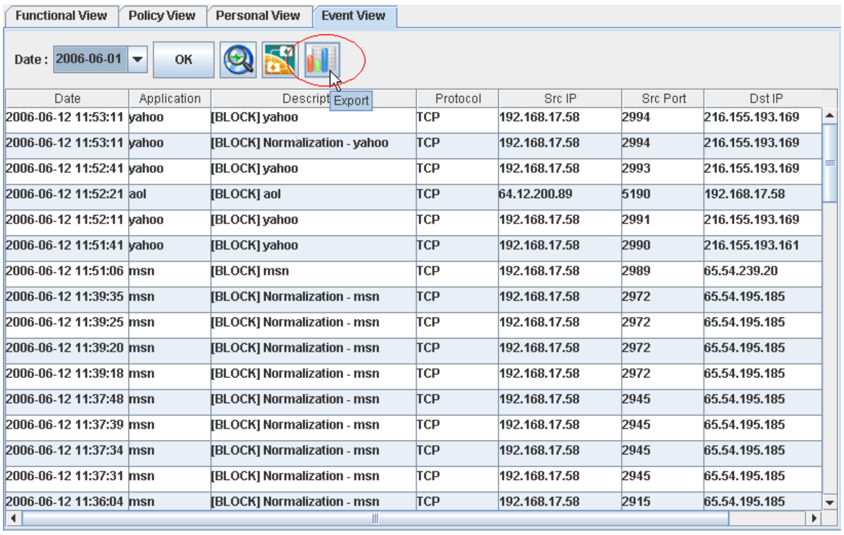


19.3.4 导出事件报表

步驟 1 导出事件报表

点击图示  进阶设定。

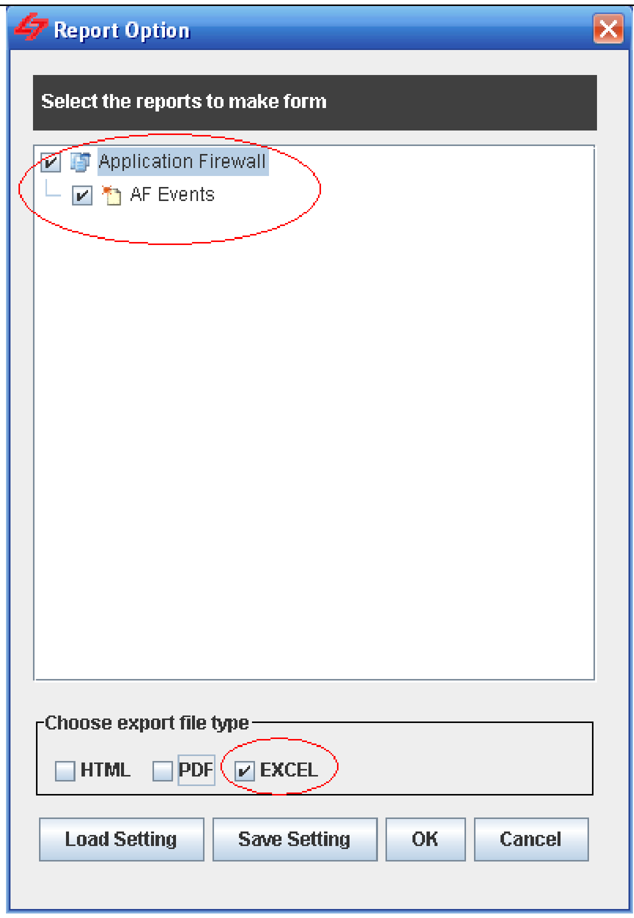
Reports > Application Firewall > Event View



步驟 2 选择导出报表的项目

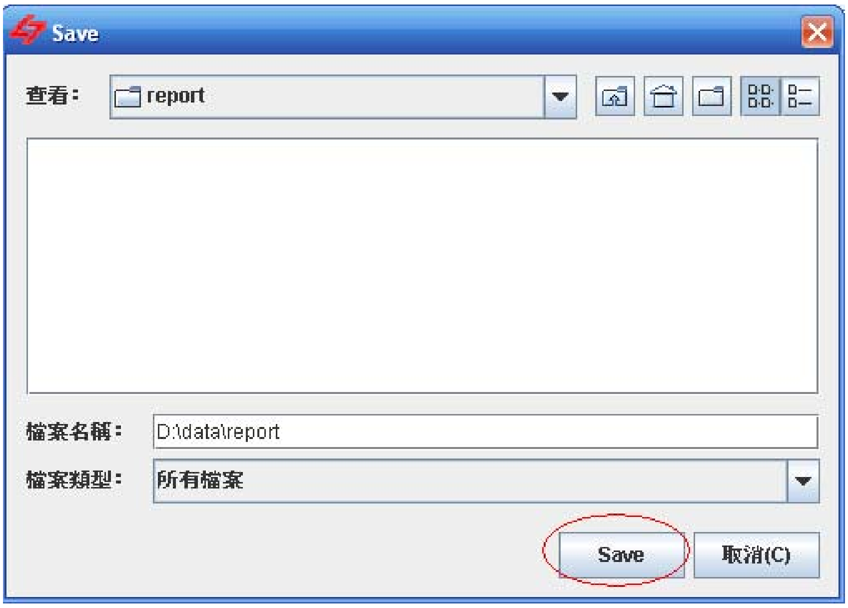
勾选您要导出的报表项目，然后勾选会出报表的类型为 Excel，点击 OK 继续。

Reports > Application Firewall > Event View > Export



字段 / 按钮	说明	范例
Application Firewall	应用层防火墙可以导出的事件记录。	AF Events
Choose export file type	选择要导出报表的格式。有三种文件类型可供选择：1) HTML 2) PDF 3) EXCEL （提供原始事件数据，可供用户自行制定报表。）	EXCEL
Button		
Load Setting	将之前已储存的报表配置文件加载。	
Save Setting	储存报表配置文件。	
OK	套用设定。	
Cancel	取消设定并关闭窗口。	

表格 19-6 应用层防火墙 - 报表导出字段说明

步驟 3 储存报表 选择您要储存报表的文件夹，然后点击 **Save** 完成设定。	**Reports > Application Firewall > Event View > Export** 

第20章
实时通讯管理员报表

本章介绍实时通讯管理员报表的应用。

20.1 需求

1. 管理人员希望知道前 10 名合法的实时通讯用户排行。
2. 管理人员希望知道合法传送档案的实时通讯用户排行。
3. 管理人员希望知道 RD “Evan” 合法使用的实时通讯行为。
4. 管理人员希望将事件记录储存成 Excel 文件，可以依据自己的需求产生其他的报表格式。

20.2 方法

1. 到 Reports > IM Manager > Funcational View > Top Allowed Users 检视图形报表。
2. 到 Reports > IM Manager > Policy View > Top Allowed Users of Service，并于进阶搜寻上勾选 Action 选择 file。
3. 到 Reports > IM Manager > Personal View > Top Allowed Services of User，并于进阶搜寻的 User 字段填入 Evan。
4. 到 Reports > IM Manager > Event View，点击 Export，选择数据导出类型为 Excel。

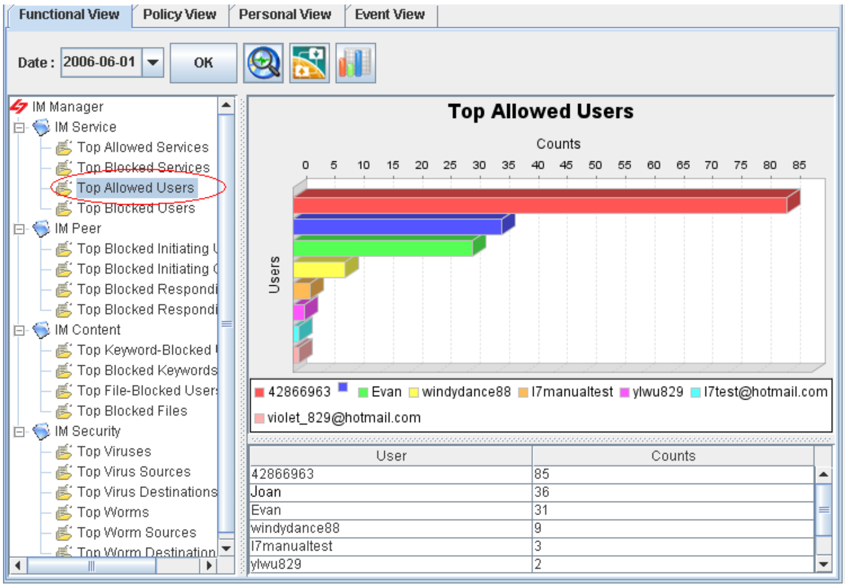
20.3 步骤

20.3.1 功能面报表浏览

步骤 1 点击被许可的使用者排行

点击 **Top Allowed Users**。

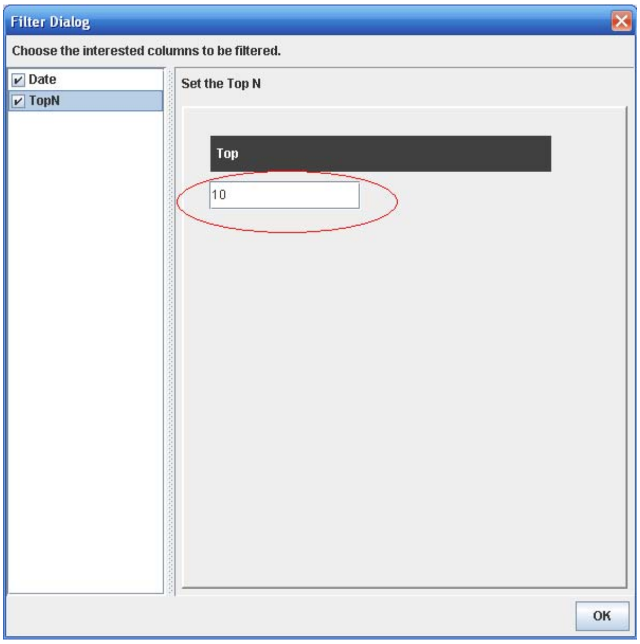
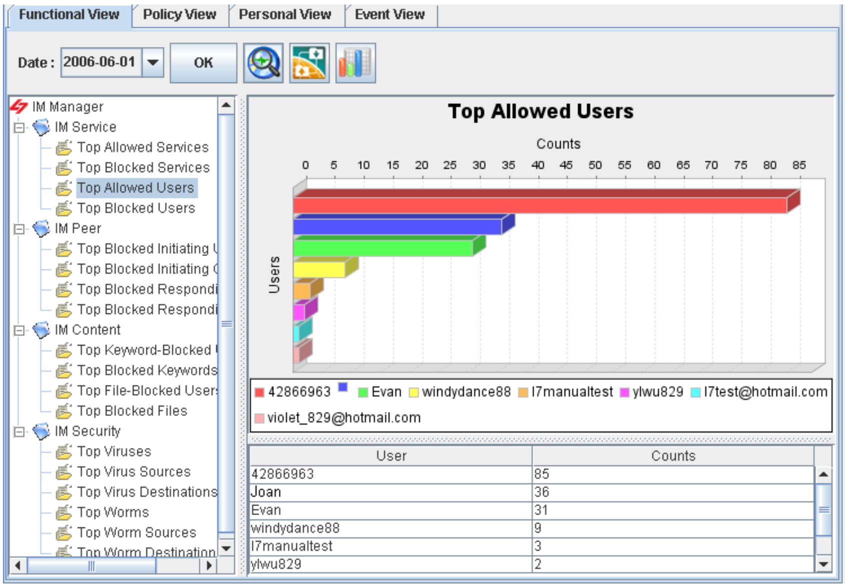
Reports > IM Manager > Functional View > Top Allowed Users



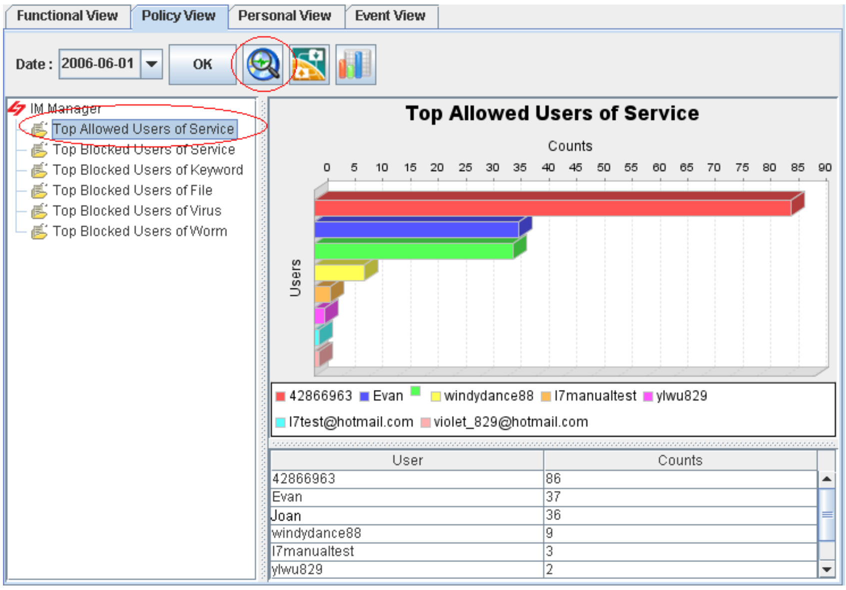
字段	说明
IM Service	依管理者所设定的实时通讯服务规则，定义其服务与使用者之间的关系。实时通讯服务报表可分成：1) 被许可的服务排行）, 2) 被拦阻的服务排行）, 3) 被许可的使用者排行, 4) 被拦阻的使用者排行。
IM Peer	依管理者所设定的实时通讯聊天对象规则，定义聊天对象彼此之间的关系。聊天对象报表可分成两

	大类：1) 因发起聊天被拦阻之使用者/群组排行）; 2) 因响应聊天被拦阻之使用者/群组排行。
IM Content	依管理者所设定的实时通讯内容过滤（关键词过滤、档案过滤），可检视非法关键词与档案的使用情形。可分成：1) 被拦阻关键词的用户排行; 2) 被拦阻的关键词排行; 3) 传送档案被拦阻的使用者排行; 4) 被拦阻的文件名排行。
IM Security	依管理者所设定的实时通讯安全防护所产生的报表，可检视病毒/蠕虫排行、遭受攻击的目的端排行，与发送病毒攻击的来源端排行。

表格 20-1 实时通讯管理员 - 报表项目说明

步驟 2 进阶搜寻报表 勾选 TopN，然后在 Top 字段上输入 10。点击 **OK** 浏览结果。	**Reports > IM Manager > Functional View > Top Allowed Users** 
步驟 3 浏览搜寻的结果 右图为前 10 名被允许的用户排名图表。	**Reports > IM Manager > Functional View > Top Allowed Users** 

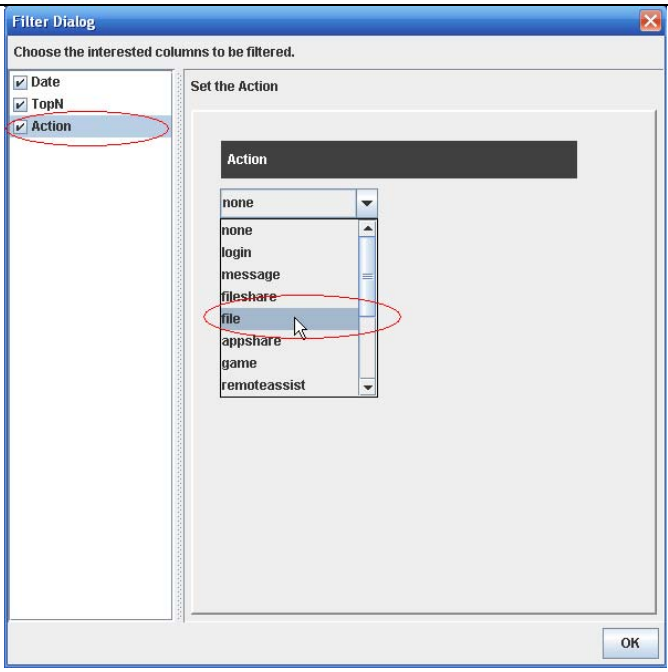
20.3.2 政策面报表浏览

步骤 1 浏览被允许使用实时通讯的用户排名 点击 **Top Allowed Users of Service**。然后点击图示  进阶设定。	**Reports > IM Manager > Policy View > Top Allowed Users of Service** 

报表项目	说明
Top Allowed Users of Service	可依搜寻的服务，查询被允许使用此服务的使用者排行。
Top Blocked Users of Service	可依搜寻的服务，查询因使用此服务而被拦阻的使用者排行。
Top Blocked Users of Keyword	可依搜寻的关键词，查询因传送讯息内容含有此关键词而被拦阻的用户排行。
Top Blocked Users of File	可依搜寻的档名，查询因传送此档名而被拦阻的使用者排行。
Top Blocked Users of Virus	可依搜寻的病毒，查询因传送/接收此病毒而被拦阻的用户排行。
Top Blocked Users of Worm	可依搜寻的蠕虫，查询因传送/接收此蠕虫而被拦阻的使用者排行。

表格 20-2 实时通讯管理员 - 政策面报表说明

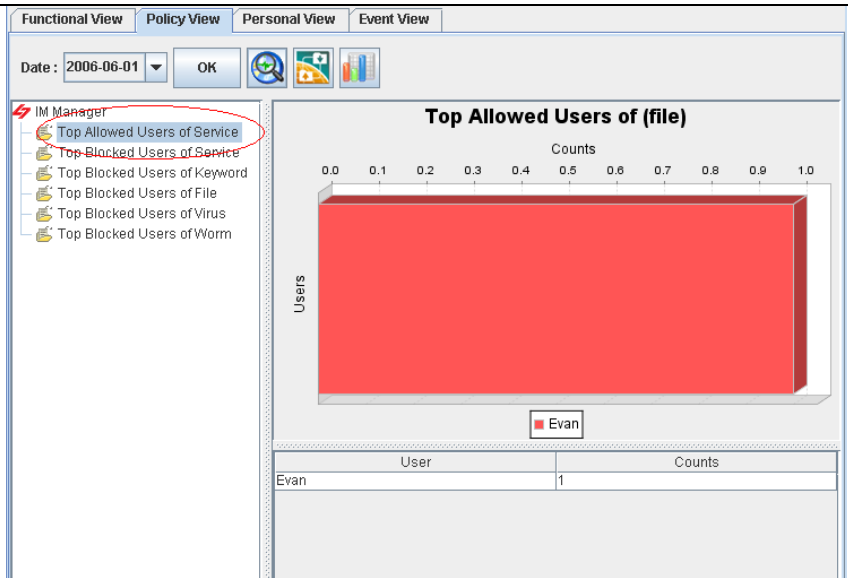
步骤 2 进阶搜寻报表 勾选 Action，然后在 Action 列表上点选 **File**。点击 **OK** 浏览结果。	**Reports > IM Manager > Policy View > Top Allowed Users of Service > Advanced**



报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为当您在管理服务器所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Action	实时通讯服务的搜寻条件。可依搜寻的实时通讯服务，查询使用此实时通讯服务而被允许/被拦阻的使用者排行。	File

表格 20-3 实时通讯管理员 - 政策面报表进阶搜寻说明

步驟 3 浏览设定的结果 右图为被允许传送档案的使用者排行。	**Reports > IM Manager > Policy View > Top Allowed Users of Service of (File)**

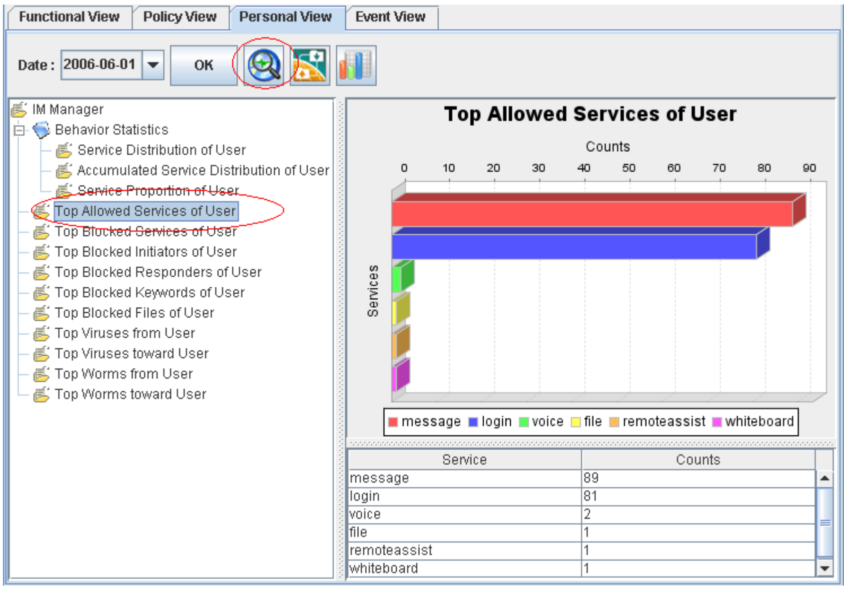


20.3.3 个人面报表浏览

步骤 1 浏览合法的实时通讯服务排行

点击 **Top Allowed Services of Users**。然后点击图示 进阶设定。

Reports > IM Manager > Personal View > Top Allowed Services of User



报表项目	说明
Behavior Statistics	可浏览所搜寻的用户，其使用实时通讯细部行为的分布状况、累积服务分布与该使用者的使用的服务比例。
Top Allowed Services of User	依搜寻的使用者，查询其合法使用的服务排行。
Top Blocked Services of User	依搜寻的使用者，查询其违法使用的服务排行。
Top Blocked Initiators of User	依搜寻的使用者，查询其因发起聊天而被拦阻的使用者排行。
Top Blocked Responders of User	依搜寻的使用者，列出因响应聊天要求而被拦阻的使用者排行。

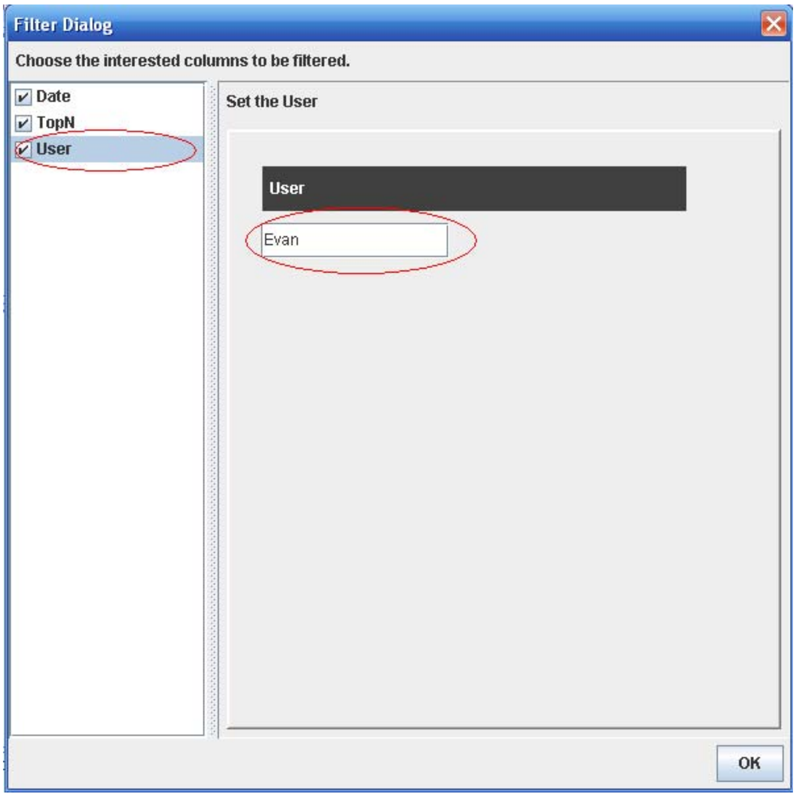
Top Blocked Keywords of User	依搜寻的用户，查询其被拦阻的关键词排行。
Top Blocked Files of User	依搜寻的使用者，查询其被拦阻的档案排行。
Top Viruses from User	依搜寻的用户，查询其发送的病毒种类排行。
Top Viruses toward User	依搜寻的用户，查询其遭受的病毒种类排行。
Top Worms from User	依搜寻的使用者，查询其发送的蠕虫种类排行。
Top Worms toward User	依搜寻的使用者，查询其遭受的蠕虫种类排行。

表格 20-4 实时通讯管理员 - 个人面报表说明

步驟 2 进阶搜寻报表

勾选 Src IP，然后在 User 字段上输入 **Evan**。点击 **OK** 浏览结果。

Reports > IM Manager > Personal View > Top Allowed Services of User > Advanced



报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为您在管理服务器时所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
User	查询使用者（在此指的是 IM User），列举此使用者所使用的合法服务排名。	192.168.17.58

表格 20-5 实时通讯管理员 - 个人面报表进阶搜寻说明

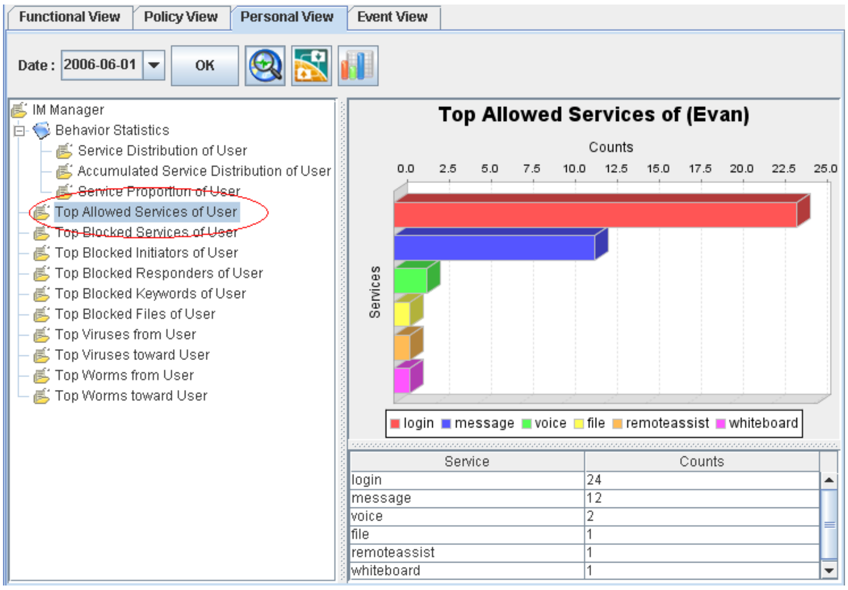
<table>
<tr><td>

步驟 3 浏览搜寻结果

右图用户 Evan 所使用的合法实时通讯服务排名。

</td><td>

Reports > IM Manager > Personal View > Top Allowed Services of (Evan)



</td></tr>
</table>

20.3.4 导出事件报表

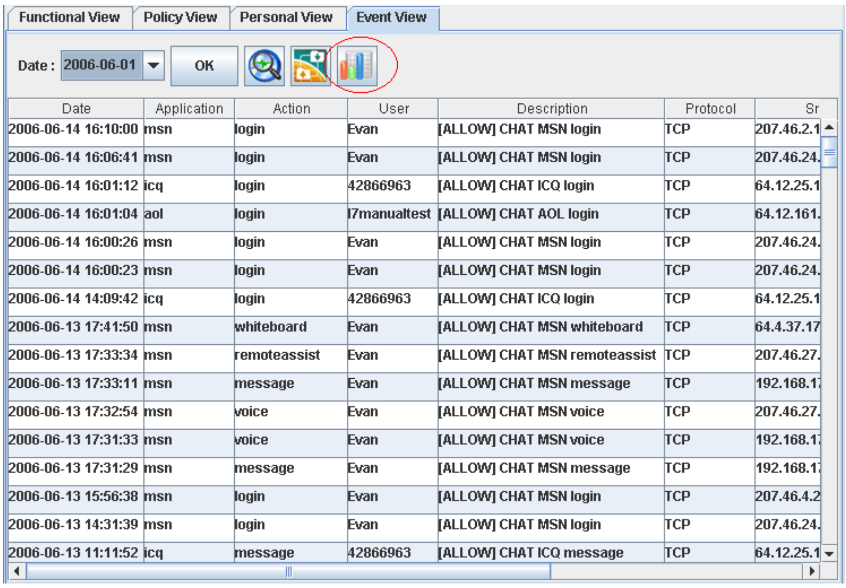
<table>
<tr><td>

步驟 1 导出事件报表

点击图示  进阶设定。

</td><td>

Reports > IM Manager > Event View



Date	Application	Action	User	Description	Protocol	Sr
2006-06-14 16:10:00	msn	login	Evan	[ALLOW] CHAT MSN login	TCP	207.46.2.1
2006-06-14 16:06:41	msn	login	Evan	[ALLOW] CHAT MSN login	TCP	207.46.24.
2006-06-14 16:01:12	icq	login	42866963	[ALLOW] CHAT ICQ login	TCP	64.12.25.1
2006-06-14 16:01:04	aol	login	l7manualtest	[ALLOW] CHAT AOL login	TCP	64.12.161.
2006-06-14 16:00:26	msn	login	Evan	[ALLOW] CHAT MSN login	TCP	207.46.24.
2006-06-14 16:00:23	msn	login	Evan	[ALLOW] CHAT MSN login	TCP	207.46.24.
2006-06-14 14:09:42	icq	login	42866963	[ALLOW] CHAT ICQ login	TCP	64.12.25.1
2006-06-13 17:41:50	msn	whiteboard	Evan	[ALLOW] CHAT MSN whiteboard	TCP	64.4.37.17
2006-06-13 17:33:34	msn	remoteassist	Evan	[ALLOW] CHAT MSN remoteassist	TCP	207.46.27.
2006-06-13 17:33:11	msn	message	Evan	[ALLOW] CHAT MSN message	TCP	192.168.1
2006-06-13 17:32:54	msn	voice	Evan	[ALLOW] CHAT MSN voice	TCP	207.46.27.
2006-06-13 17:31:33	msn	voice	Evan	[ALLOW] CHAT MSN voice	TCP	192.168.1
2006-06-13 17:31:29	msn	message	Evan	[ALLOW] CHAT MSN message	TCP	192.168.1
2006-06-13 15:56:38	msn	login	Evan	[ALLOW] CHAT MSN login	TCP	207.46.4.2
2006-06-13 14:31:39	msn	login	Evan	[ALLOW] CHAT MSN login	TCP	207.46.24.
2006-06-13 11:11:52	icq	message	42866963	[ALLOW] CHAT ICQ message	TCP	64.12.25.1

</td></tr>
<tr><td>

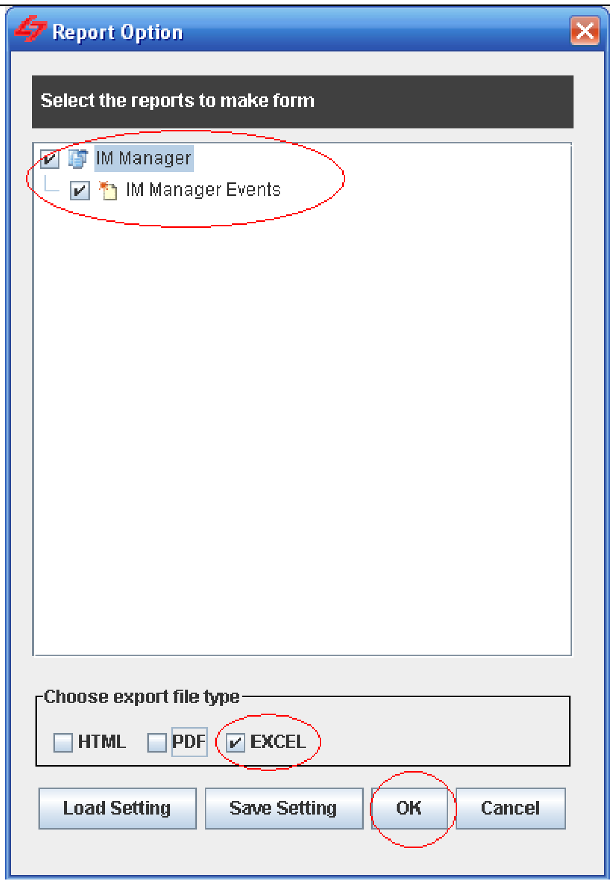
步驟 2 选择导出报表的项目

勾选您要导出的报表项目，然后勾选会出报表的类型为 Excel，点击 OK 继续。

</td><td>

Reports > IM Manager > Event View > Export

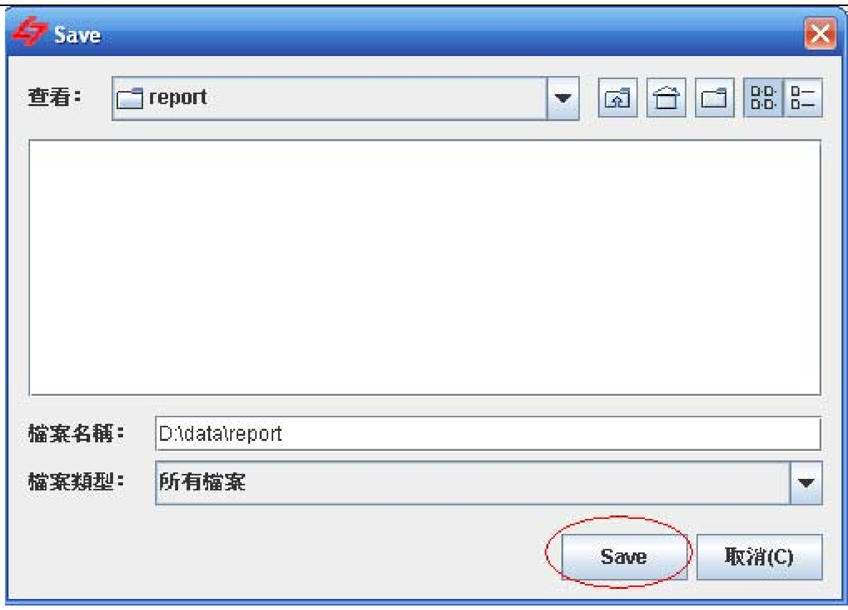
</td></tr>
</table>



字段 / 按钮	说明	范例
IM Manager	实时通讯管理员可以导出的事件记录。	AF Events
Choose export file type	选择要导出报表的格式。有三种文件类型可供选择：1) HTML 2) PDF 3) EXCEL （提供原始事件数据，可供用户自行制定报表。）	EXCEL
Button		
Load Setting	将之前已储存的报表配置文件加载。	
Save Setting	储存报表配置文件。	
OK	套用设定。	
Cancel	取消设定并关闭窗口。	

表格 20-6 实时通讯管理员 - 报表导出字段说明

步骤 3 储存报表 选择您要储存报表的文件夹，然后点击 **Save** 完成设定。	**Reports > IM Manager > Event View > Export**

Save
查看：
report
檔案名稱：
D:\data\report
檔案類型：
所有檔案
Save
取消(C)

第21章
网页管理员报表

本章节介绍网页管理员报表的应用。

21.1 需求

1. 管理人员希望知道前 10 名存取网站排名。
2. 管理人员希望知道因违反网页管理员政策的控管类别（content_object）而被拦阻的网站排名。
3. 管理人员希望知道 192.168.17.58 这台计算机到目前为止的前 10 名存取网页排名。
4. 管理人员希望将事件记录储存成 Excel 文件，可以依据自己的需求产生其他的报表格式。

21.2 方法

1. 到 Reports > Web Manager > Funcational View > Top Access Sites 检视图形报表。
2. 到 Reports > Web Manager > Policy View > Top Blocked Sites of Reason，并于进阶搜寻上勾选 Function Type 选择 content_object。
3. 到 Reports > Web Manager > Personal View > Top Access Sites of User，并于进阶搜寻的 Src IP 字段填入 192.168.17.58。
4. 到 Reports > Web Manager > Event View，点击 Export，选择数据导出类型为 Excel。

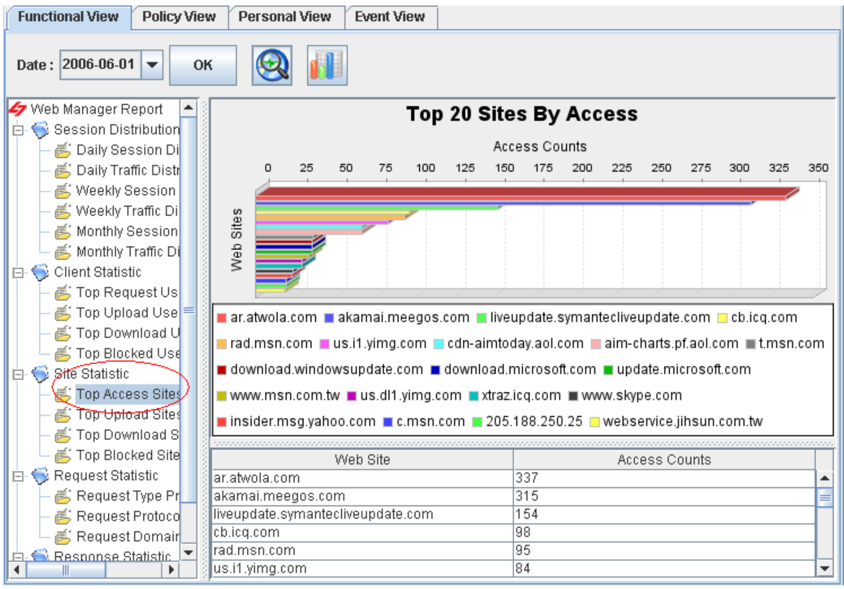
21.3 步骤

21.3.1 功能面报表浏览

步驟 1 点击存取网站排名项目

点击 **Top Access Sites**。

Reports > Web Manager > Functional View > Top Access Sites



项目	说明
Session Distribution	可查询每日、每周、每月的浏览/回应网页的联机次数与流量分布状况。每日以 24 小时为单位，每周与每月皆以日期为单位。

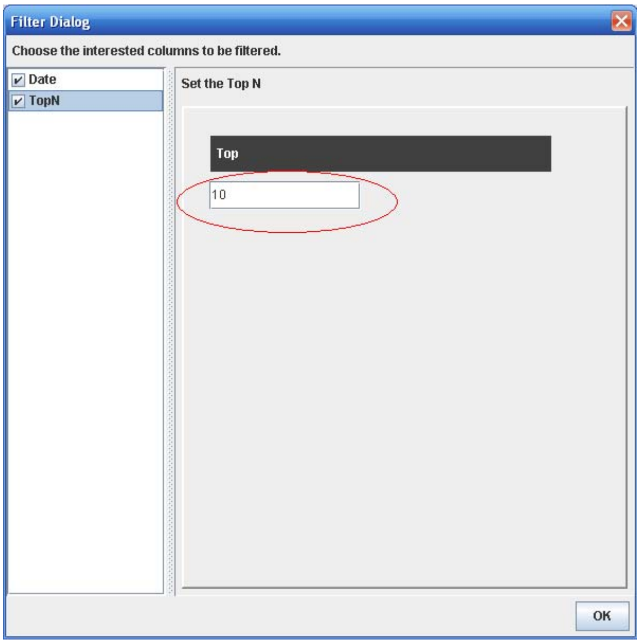
Client Statistic	可查询网页浏览网页/上传/下载与因浏览网页而被拦阻的使用者排行。
Site Statistic	可查询热门存取网站/上传网站/下载网站/被拦阻的网站排行。
Request Statistic	可查询网页浏览的访问方法/通讯协议/网域等的比例。
Response Statistic	可查询网页响应内容型别/流量等的比例。

表格 21-1 网页管理员 - 功能面报表项目说明

步骤 2 进阶搜寻报表

勾选 TopN，然后在 Top 字段上输入 10。点击 **OK** 浏览结果。

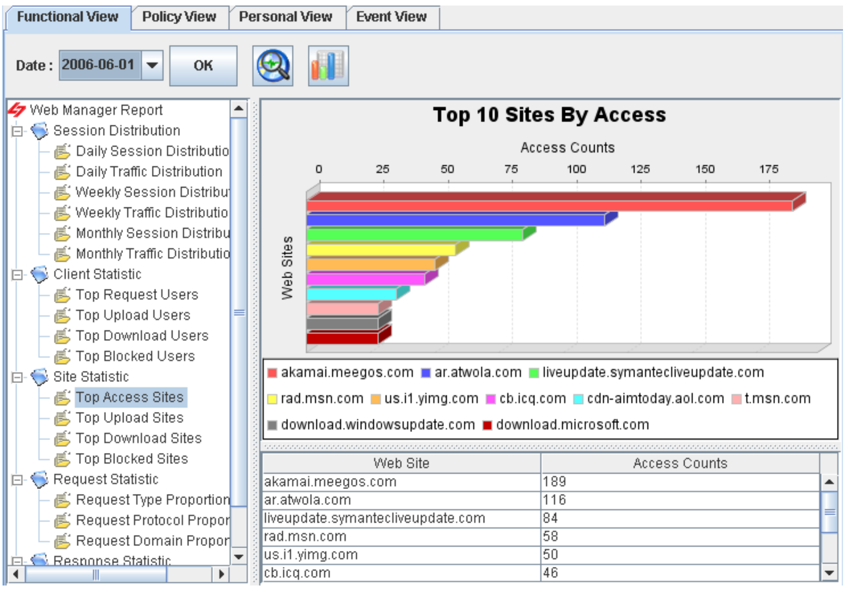
Reports > Web Manager > Functional View > Top Access Sites



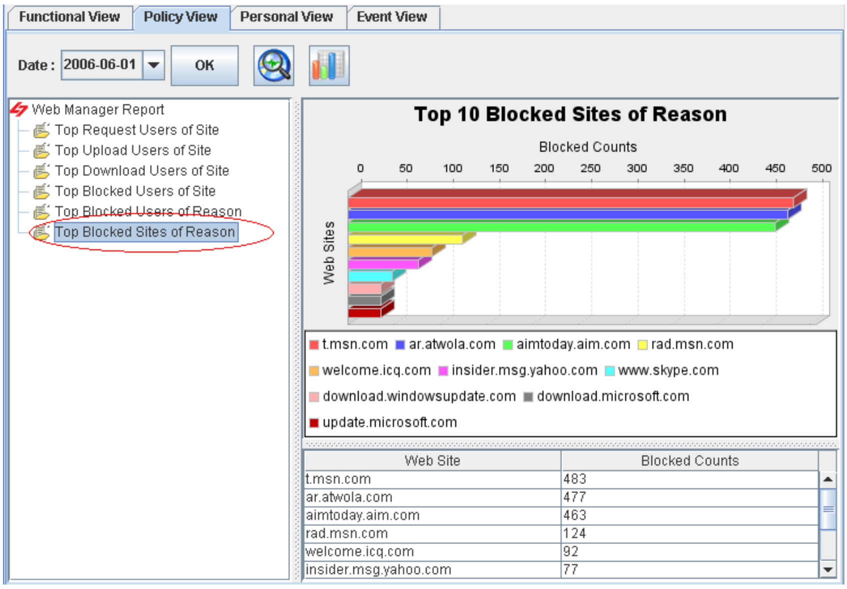
步骤 3 浏览搜寻的结果

右图为前 **10** 名被允许的用户排名图表。

Reports > Web Manager > Functional View > Top Access Sites



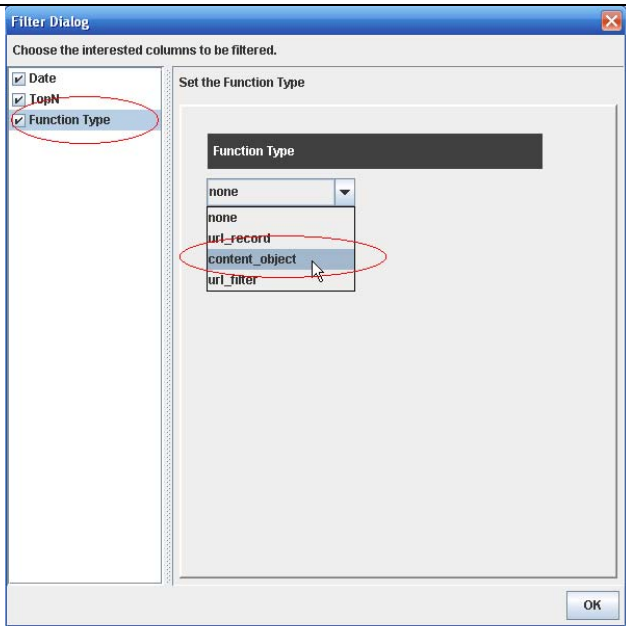
21.3.2 政策面报表浏览

步驟 1 浏览被拦阻的网站排名 点击 **Top Blocked Sites of Reason**。然后点击图示 进阶设定。	**Reports > Web Manager > Policy View > Top Blocked Sites of Reason** 

报表项目	说明
Top Request Users of Site	可依搜寻的网站，查询经常浏览此网站的使用者排行。
Top Upload Users of Site	可依搜寻的网站，查询经常上传此网站的使用者排行。
Top Download Users of Site	可依搜寻的网站，查询经常下载此网站的使用者排行。
Top Blocked Users of Site	可依搜寻的网站，查询因浏览此网站而被拦阻的使用者排行。
Top Blocked Users of Reason	可依搜寻的控管类别，查询因违反此控管类别政策而被拦阻的使用者排行。
Top Blocked Sites of Reason	可依搜寻的控管类别，查询因违反此控管类别政策的网站排行。

表格 21-2 网页管理员 - 政策面报表说明

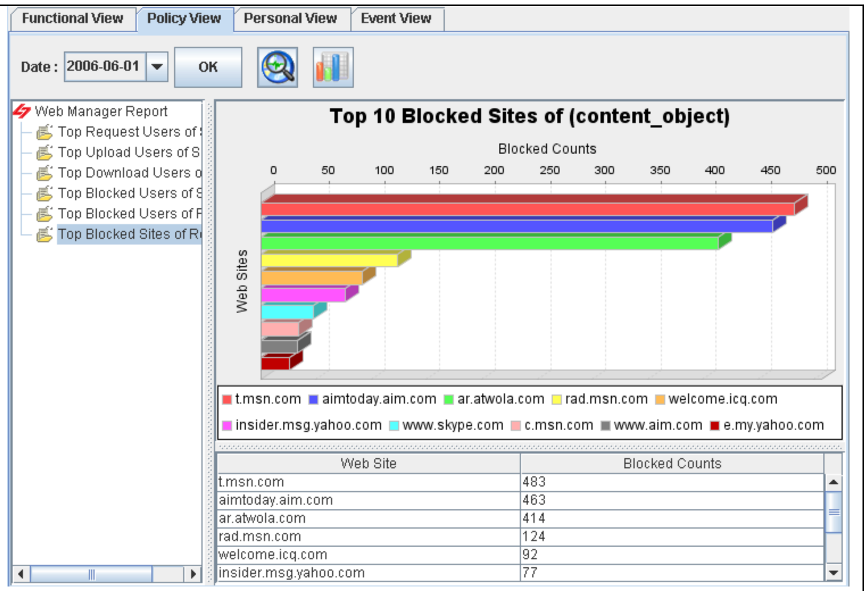
步驟 2 进阶搜寻报表 勾选 Function Type，然后在 Function Type 列表上点选 **content_object**。点击 **OK** 浏览结果。	**Reports > Web Manager > Policy View > Top Blocked Sites of Reason > Advanced**



报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为当您在管理服务器所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Function Type	网页管理员报表的细部搜寻条件。可依搜寻的控管类别（Function Type），查询所有违反控管类别政策的网站排名。	content_object

表格 21-3 网页管理员政策 - 面报表进阶搜寻说明

步驟 3 浏览设定的结果 右图为因违反控管类别政策而被拦阻的网站排名。	**Reports > Web Manager > Policy View > Top Blocked Sites of Reason**

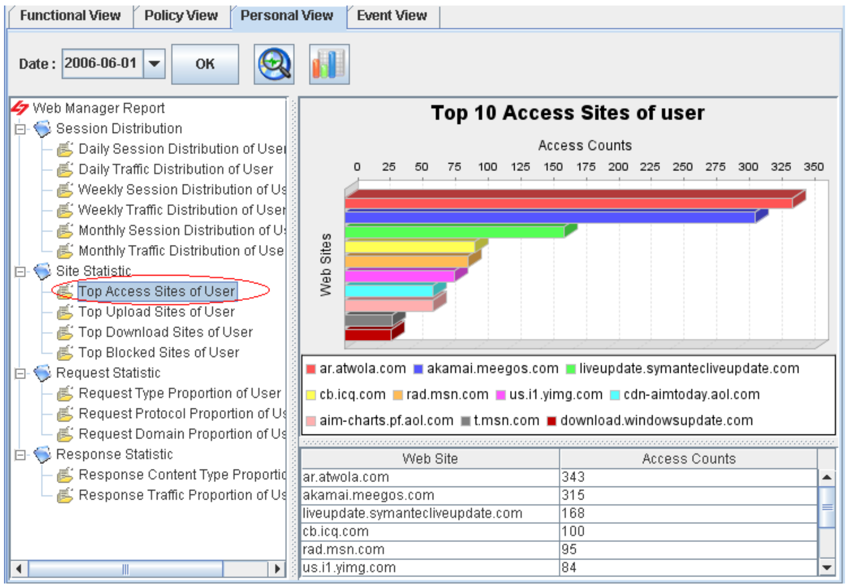


21.3.3 个人面报表浏览

步驟 1 浏览使用者经常存取的网站排行

点击 **Top Allowed Services of Users**。然后点击图示 进阶设定。

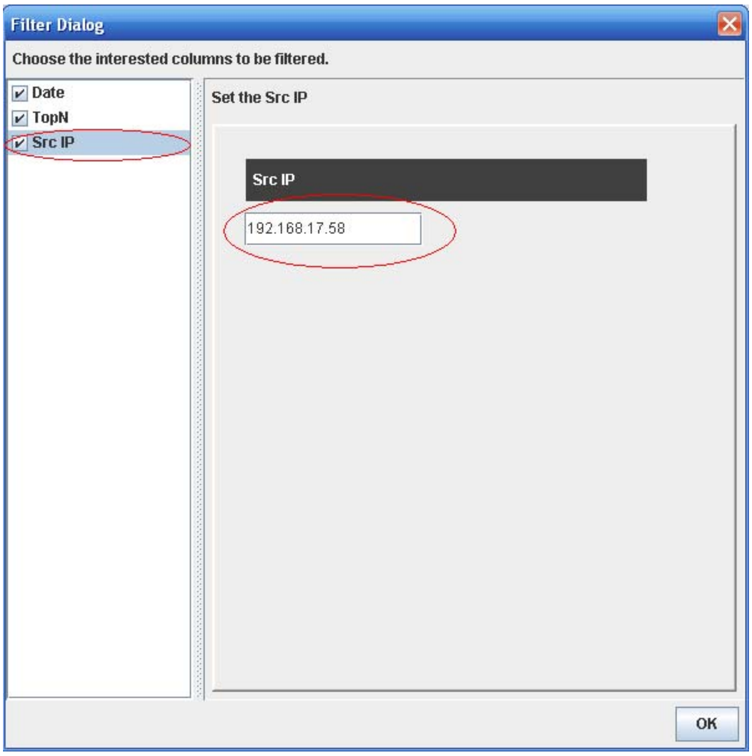
Reports > Web Manager > Personal View > Top Access Sites of User



报表项目	说明
Session Distribution of User	可依搜寻的使用者（IP），查询此使用者每日、每周、每月的浏览/响应网页的联机次数与流量分布状况。每日以 24 小时为单位，每周与每月皆以日期为单位。
Site Statistic	可依搜寻的使用者（IP），查询此使用者存取网站/上传/下载与浏览违法的网站排行。
Request Statistic	可依搜寻的使用者（IP），查询此使用者经常存取网站/上传网站/下载网站/被拦阻的网站排行。
Response Statistic	可依搜寻的使用者（IP），查询此使用者网页浏览的访问方法/通讯协议/网域等的

	比例。

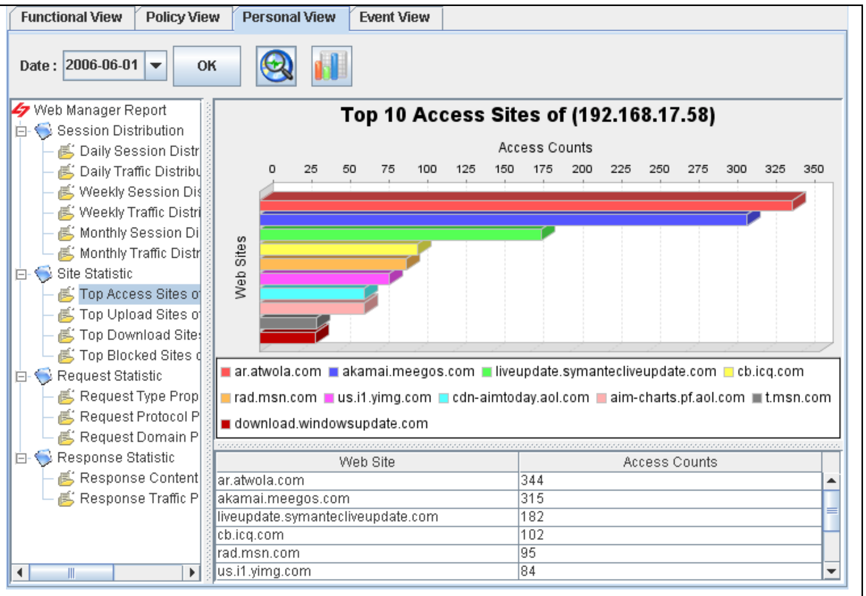
表格 21-4 网页管理员 - 个人面报表说明

步驟 2 进阶搜寻报表 勾选 Src IP，然后在 Src IP 字段上输入 **192.168.17.58**。点击 **OK** 浏览结果。	**Reports > Web Manager > Personal View > Top Access Sites of User > Advanced** 

报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为您在管理服务器所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Src	查询使用者（在此指的是使用者的 IP），查询此使用者的存取网站排行。	192.168.17.58

表格 21-5 网页管理员 - 个人面报表进阶搜寻说明

步驟 3 浏览搜寻结果 右图为使用者 192.168.17.58 的存取网站排行。	**Reports > Web Manager > Personal View > Top Access Sites of User**

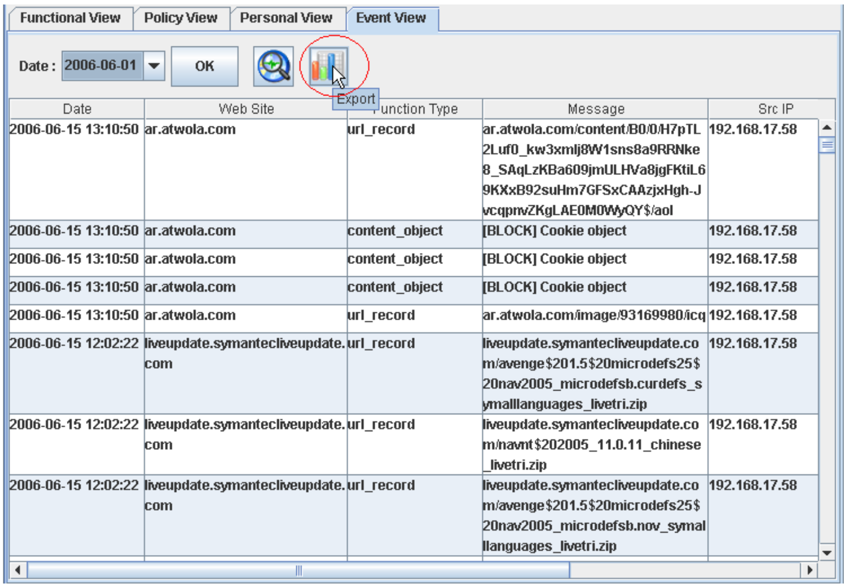


21.3.4 导出事件报表

步驟 1 导出事件报表

点击图示  进阶设定。

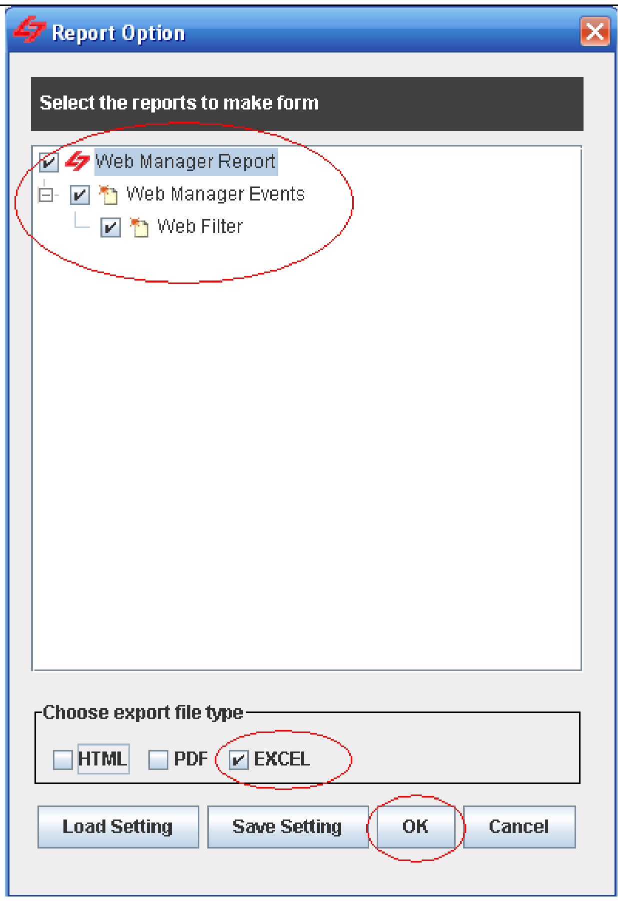
Reports > Web Manager > Event View



步驟 2 选择导出报表的项目

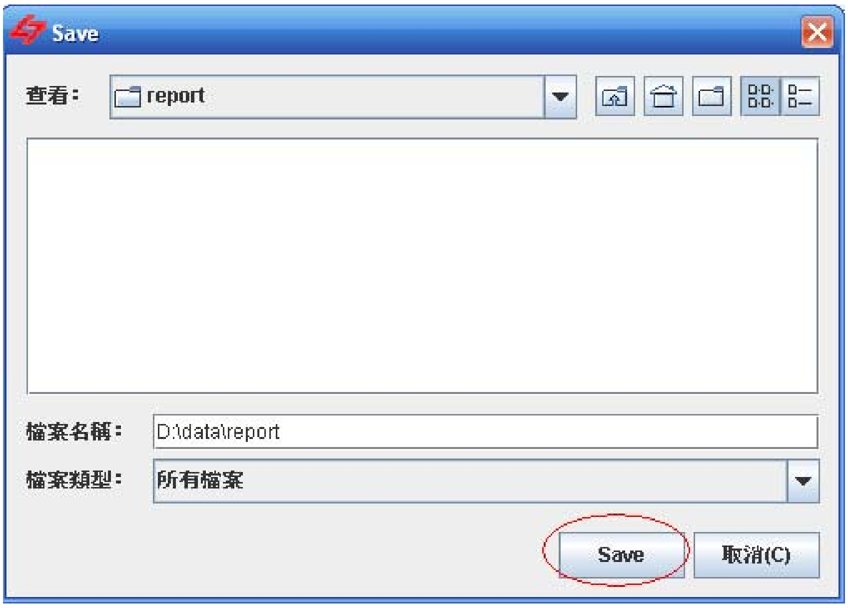
勾选您要导出的报表项目，然后勾选会出报表的类型为 Excel，点击 OK 继续。

Reports > Web Manager > Event View > Export



字段 / 按钮	说明	范例
Web Manager	网页管理员可以导出的事件记录。	Web Manager Events Web Filter
Choose export file type	选择要导出报表的格式。有三种文件类型可供选择：1) HTML 2) PDF 3) EXCEL （提供原始事件数据，可供用户自行制定报表。）	EXCEL
Button		
Load Setting	将之前已储存的报表配置文件加载。	
Save Setting	储存报表配置文件。	
OK	套用设定。	
Cancel	取消设定并关闭窗口。	

表格 21-6 网页管理员 - 报表导出字段说明

步驟 3 储存报表 选择您要储存报表的文件夹，然后点击 **Save** 完成设定。	**Reports > Web Manager > Event View > Export** 

第22章
流量管理员报表

本章节介绍流量管理员报表的应用。

22.1 需求

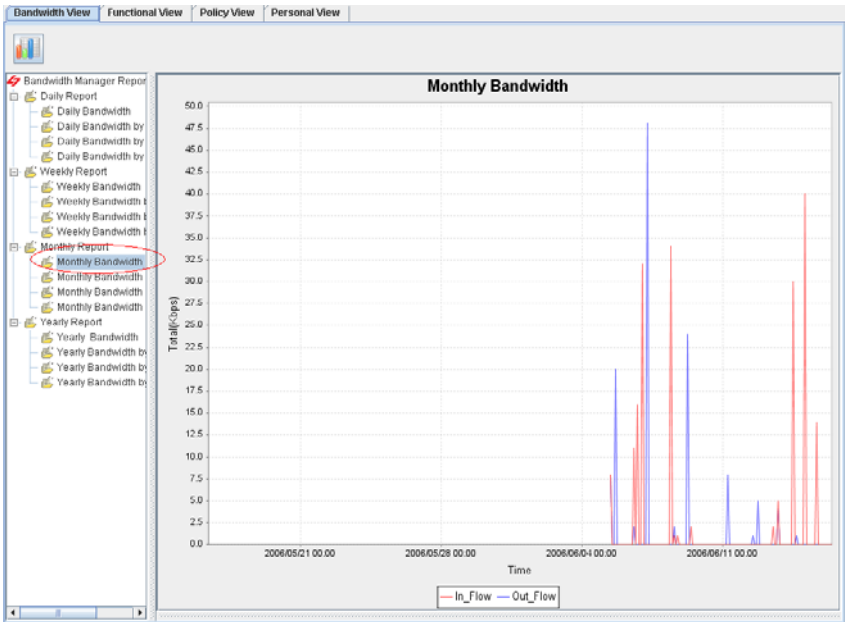
1. 管理人员希望知道 2006 年 6 月份的带宽使用状况。
2. 管理人员希望知道 2006 年 6 月 15 日网络进出总流量最大的前 5 名使用者排行。
3. 管理人员希望知道 2006 年 6 月 15 日使用 FTP 与 HTTP 等应用软件的最大总流量之使用者排行。
4. 管理人员希望知道 2006 年 6 月 15 日使用者（192.168.17.58）使用的应用软件之最大总流量排行。

22.2 方法

1. 到 Reports > Traffic Manager > Bandwidth View > Monthly Report > Monthly Bandwidth 检视图形报表。
2. 到 Reports > Traffic Manager > Functional View > Daily Totoal Traffic > Daily Top Total Traffic by User，并于进阶搜寻上的 TopN 字段上填入 5。
3. 到 Reports > Traffic Manager > Policy View > Daily Top Total Traffic by User of Application，并于进阶搜寻的 Application 字段选择 ftp 与 http。
4. 到 Reports > Traffic Manager > Personal View > Daily Top Total Traffic by Application of User，并于进阶搜寻上勾选 Sip，然后填入 IP 地址 192.168.17.58。

22.3 步骤

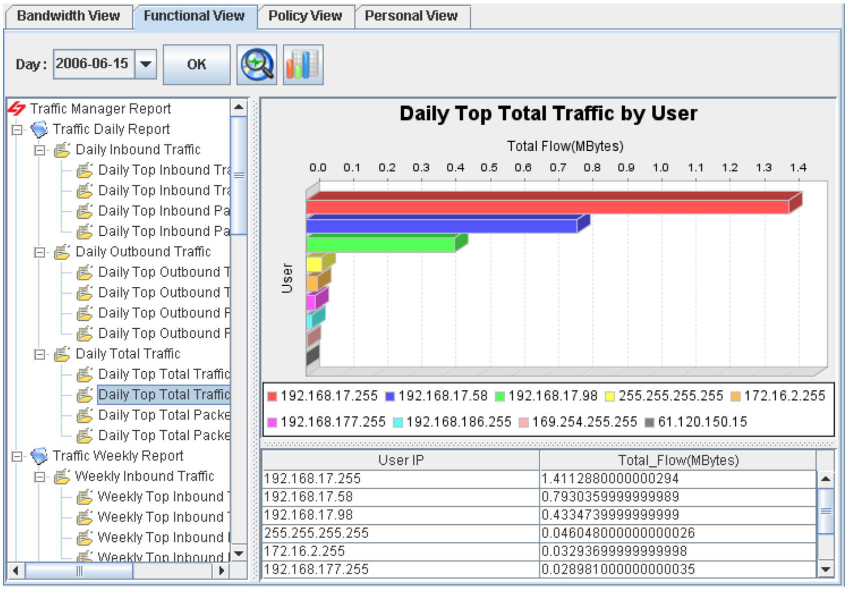
22.3.1 带宽面报表浏览

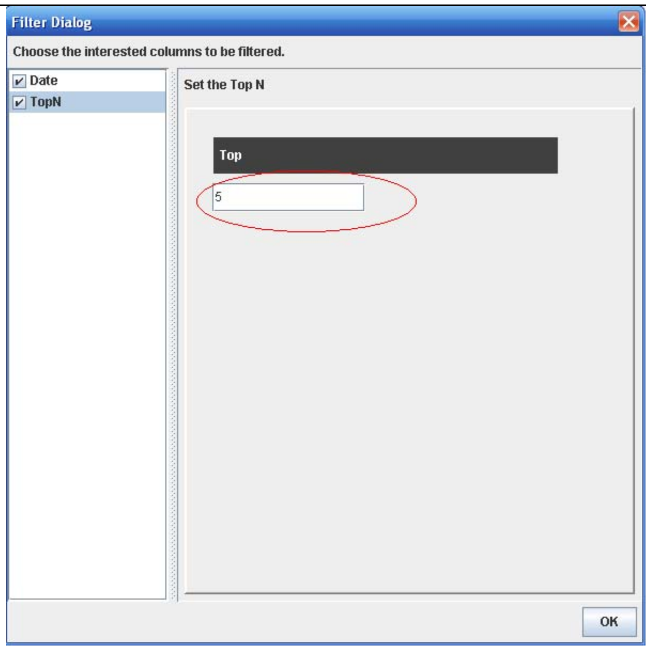
步骤 1 点击每月带宽折线图 点击 Monthly Bandwidth。	**Reports > Traffic Manager > Bandwidth View > Monthly Report > Monthly Bandwidth** 

字段	说明
Daily Report	查询每日带宽状况，依应用程序/带宽类别/应用程序类别等分类方式，方便查询对内带宽/对外带宽/总带宽的流量。
Weekly Report	查询每周带宽状况，依应用程序/带宽类别/应用程序类别等分类方式，方便查询对内带宽/对外带宽/总带宽的流量。
Monthly Report	查询每月带宽状况，依应用程序/带宽类别/应用程序类别等分类方式，方便查询对内带宽/对外带宽/总带宽的流量。
Yearly Report	查询每年带宽状况，依应用程序/带宽类别/应用程序类别等分类方式，方便查询对内带宽/对外带宽/总带宽的流量。

表格 22-1 流量管理员 - 带宽面报表项目说明

22.3.2 功能面报表浏览

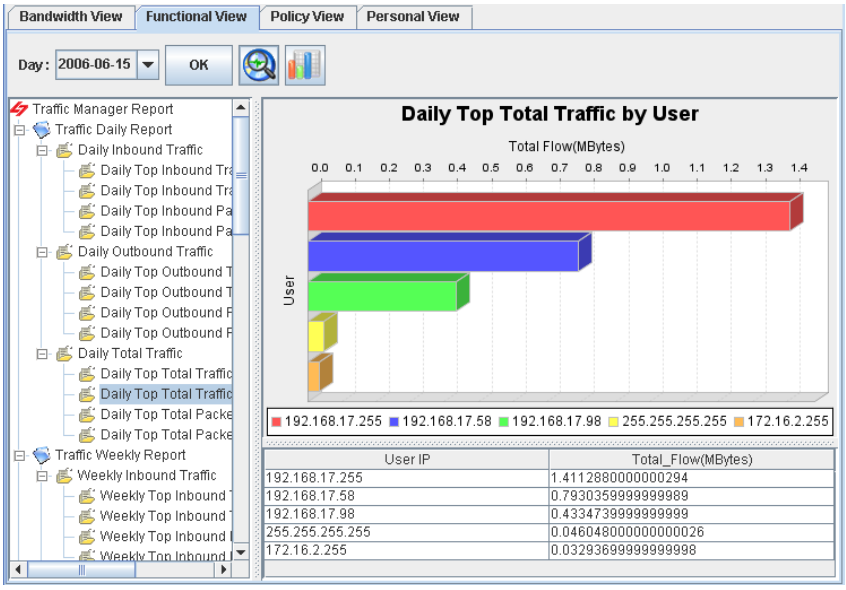
步驟 1 点击每日最大流量之使用者排行 在工具栏上的 Day 字段选择 2006-06-15，点击 **OK** 继续。点击 **Daily Top Total Traffic by User**，然后点击图示 进阶设定。	**Reports > Traffic Manager > Functional View > Daily Traffic Report > Daily Totoal Traffic > Daily Top Total Traffic by User** 
步驟 2 进阶搜寻报表 勾选 TopN，然后在 Top 字段上输入 5。点击 **OK** 浏览结果。	**Reports > Traffic Manager > Functional View > Daily Traffic Report > Daily Totoal Traffic > Daily Top Total Traffic by User**



步驟 3 浏览搜寻的结果

右图为前 5 总流量最大的使用者排名。

Reports > Traffic Manager > Functional View > Daily Traffic Report > Daily Totoal Traffic > Daily Top Total Traffic by User

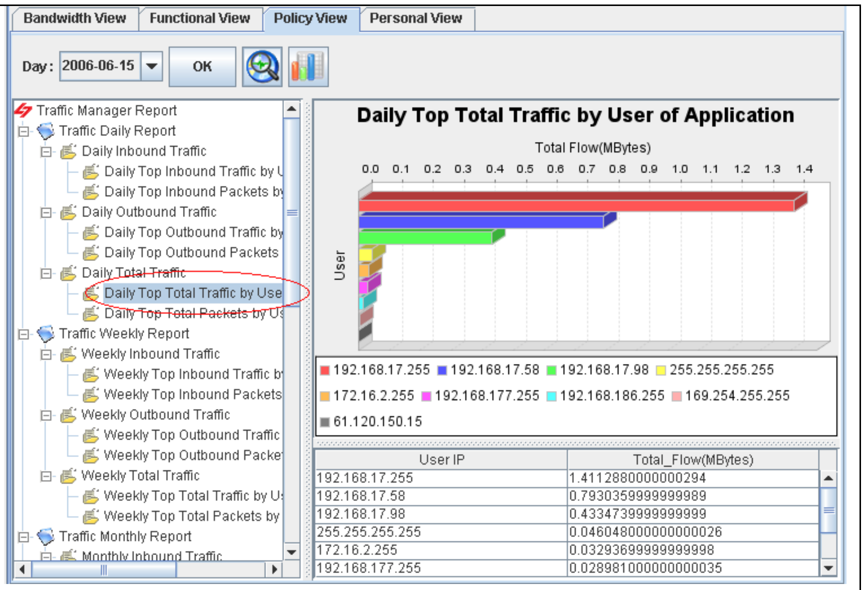


22.3.3 政策面报表浏览

步驟 1 浏览每日应用程序流量最大的用户排行

点击 **Daily Top Total Traffic by User of Application**。然后点击图示 进阶设定。

Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application



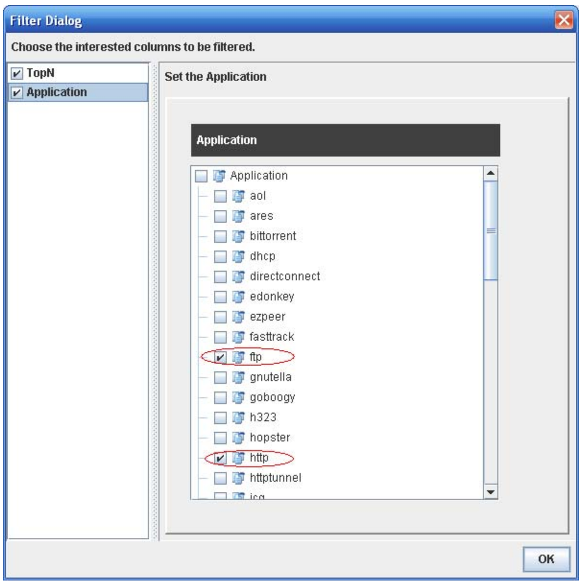
报表项目	说明
Traffic Daily Report	可查询每日流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Weekly Report	可查询每周流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Monthly Report	可查询每月流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Quarterly Report	可查询每季流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Yearly Report	可查询每年流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。

表格 22-2 流量管理员 - 政策面报表说明

步驟 2 进阶搜寻报表

勾选 Application，然后在 Application 列表上勾选 **ftp** 与 **http**。点击 **OK** 浏览结果。

Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application



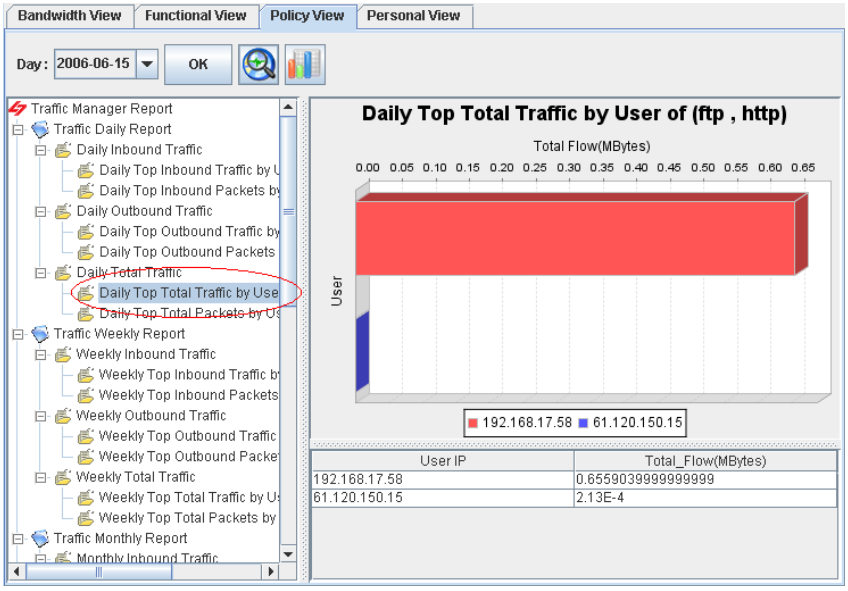
报表项目	说明	范例
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Application	应用软件的搜寻条件。可依搜寻的应用软件，查询使用此实时应用软件的用户排行。（可复选）	File

表格 22-3 流量管理员 - 政策面报表进阶搜寻说明

步驟 3 浏览设定的结果

右图为最常使用 ftp 与 http 应用软件的用户排行。

Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application

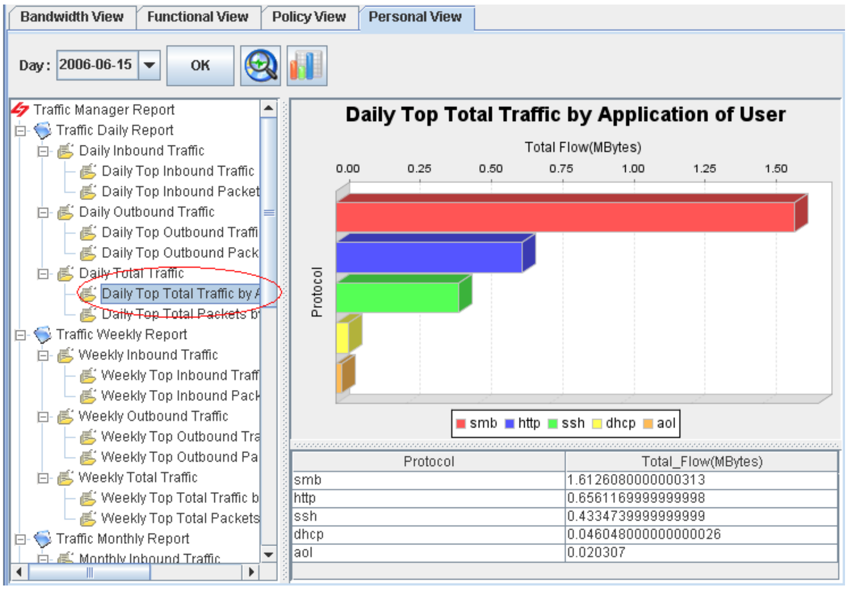


22.3.4 个人面报表浏览

步驟 1 浏览用户应用软件的流量排行

点击 **Daily Top Total Traffic by Application of User**。然后点击图示 进阶设定。

Reports > Traffic Manager > Personal View > Traffic Daily Report > Daily Total Traffic > Daily Top Total Traffic by Application of User



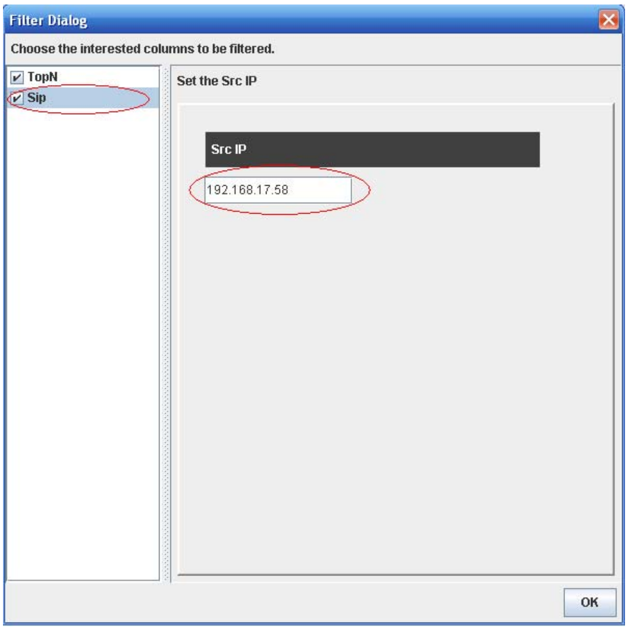
报表项目	说明
Traffic Daily Report	可依选择的使用者，查询其每日流量与封包数的对内/对外/总流量/总封包数排行与应用软件排行。
Traffic Weekly Report	可依选择的使用者，查询其每周流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Monthly Report	可依选择的使用者，查询其每月流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Quarterly Report	可依选择的使用者，查询其每季流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。
Traffic Yearly Report	可依选择的使用者，查询其每年流量与封包数的对内/对外/总流量/总封包数的用户排行与应用软件排行。

表格 22-4 流量管理员 - 个人面报表说明

步驟 2 进阶搜寻报表

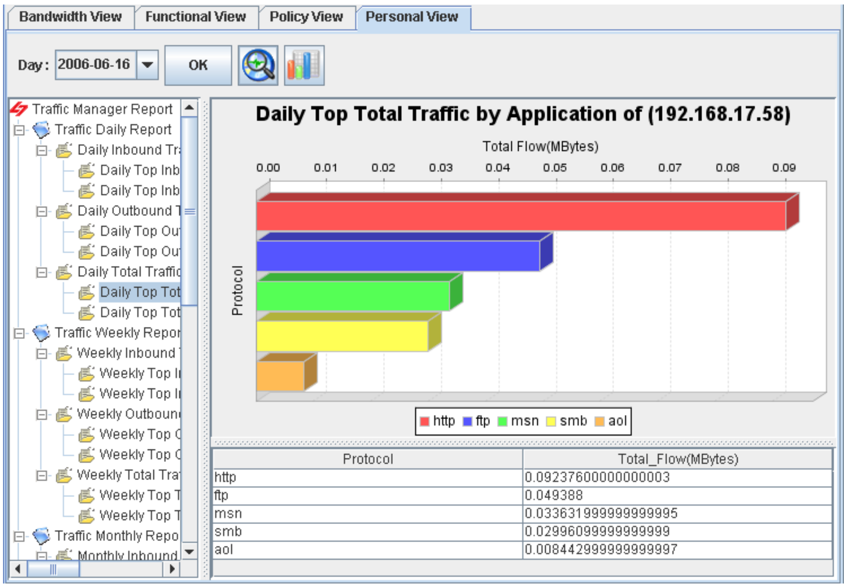
勾选 Src IP （Source IP），然后在 User 字段上输入 **Evan**。点击 **OK** 浏览结果。

Reports > IM Manager > Personal View > Top Allowed Services of User > Advanced



报表项目	说明	范例
Date	可设定要搜寻的数据之期间。注意，这个期间的有效范围为您在管理服务器时所设定的数据分割周期，超过数据分割周期的期间设定是无效的。也就是当您所设定的数据分割周期为每个月分割一个表格，您所选择的搜寻期间就不可以超过该月的范围。预设上，这个日期期间会依当周的日期为主，如果您在报表画面上看不到过去的图表，请在此选择适当的日期。	2006/06/01 ~ 2006/06/30
TopN	您在报表画面上希望看到的排行数。如果您希望只看前 10 笔，请填入 10。	10
Sip	查询使用者（在此指的是来源端的 IP 地址），查询此用户所使用的应用软件流量排行。	192.168.17.58

表格 22-5 流量管理员 - 个人面报表进阶搜寻说明

步驟 3 浏览搜寻结果 右图用户 Evan 所使用的合法实时通讯服务排名。	**Reports > Application Firewall > Personal View > Top Blocked Protocols of User** 

第10部

侧录稽核

第23章
侧录稽核

本章节介绍实时通讯与网页的侧录。

23.1 需求

为符合 BS7799 的规范，帮助企业执行 BS7799 计划，InstantScan 阶层式管理与稽核系统能够保护用户的隐私，免于一般人随便浏览其聊天信息。然而，当有泄密情况发生时，这些测录资料亦可供稽核人员随时采证，防范员工不法的举动而危及公司。所以只有管理人员与稽核人员可以看到侧录的内容，网管人员只可以设定 InstantScan，无法进入侧录系统。目前侧录共有两大类：

1) 实时通讯内容侧录：用户使用的实时通讯软件 MSN/Yahoo/ICQ/AOL 皆可实时侧录传送的讯息与档案，并以红字标示违法的关键词与传文件文件名。
2) 网页网址侧录：使用者浏览的网页实时侧录。可以查询使用者浏览网页的状况与其合法性。

23.2 方法

1. 到 Auditor > IM Recorder 检视侧录内容。
2. 到 Auditor > Web Recorder 检视侧录内容。

23.3 步骤

23.3.1 实时通讯内容侧录

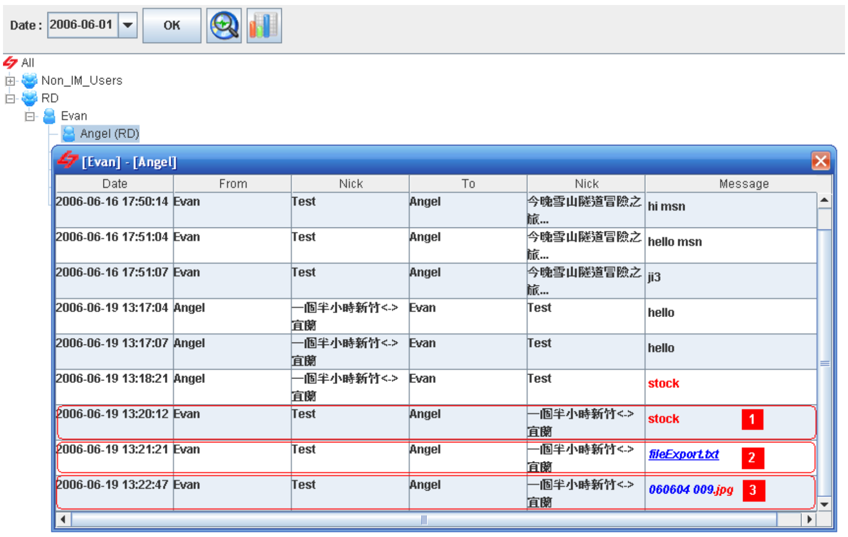
步骤 4 实时通讯内容侧录

只有管理人员与稽核人员可以看到侧录内容。当您打开实时通讯侧录器后，将有类似右图的讯息显示。实时通讯侧录器以树状结构显示。第一层为群组，第二层为在此群组内的使用者，第三者为与此用户聊天的对象，第四层为侧录到的讯息。如果您已经设定用户规则，经由同一用户规则内的所有账号所传送/ 接收的讯息内容都会显示在同一个窗口内。当用户不在实时通讯用户群组内时，将会以 Non_IM_Users 显示，所有侧录到的讯息会依用户的实时通讯账号逐条显示。

侧录如右图所示：

1. 关键词过滤：关键词以红字显示。
2. 档案传送：可将鼠标移到文件名上，点一下档案，将其储存在本地端计算机上，并开启浏览。
3. 档案过滤：违反档案传送规则的文件名会以红字显示，并禁止用户传档。

Auditor > IM Recorder

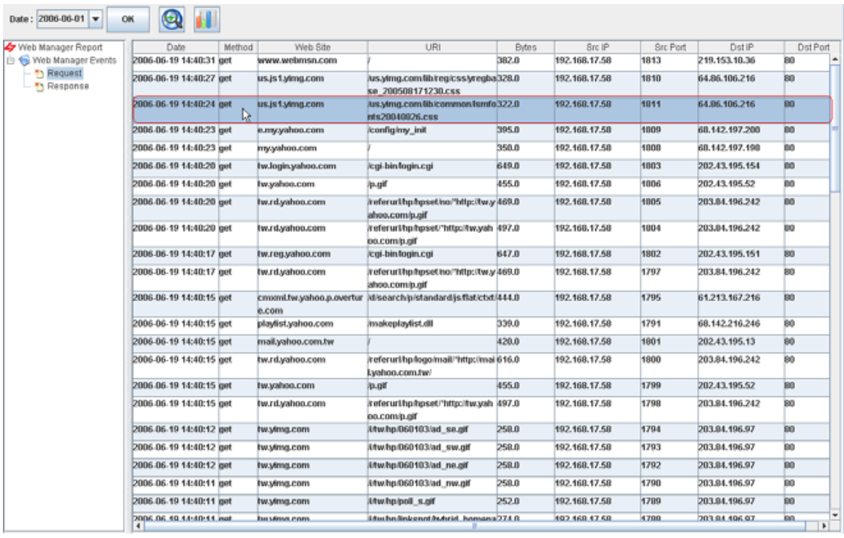


字段	说明	范例
Date	传送讯息的日期与时间。	2006-06-19 13:20:12
From	传送讯息的用户。当您在 IM User 上已有设定此使用者，则在此字段会显示您所设定的用户名称，否则将显示实时通讯账号。	Evan
Nick	传送讯息的用户的昵称。此昵称为您在 MSN 实时通讯账号所设定的	Test

（只适用 MSN）	显示名称。	
To	接收讯息的用户。当您在 IM User 上已有设定此使用者，则在此字段会显示您所设定的用户名称，否则将显示实时通讯账号。	Angel
Nick （只适用 MSN）	接收讯息的用户的昵称。此昵称为您在 MSN 实时通讯账号所设定的显示名称。	一个半小时新竹<->宜兰
Message	实时通讯讯息内容。	stock

表格 23-1 实时通讯侧录内容字段说明

23.3.2 网页内容侧录

步骤 1 浏览的网页侧录 当您在 Web Manager > Status 页面上开启 URL Recorder，所有您要浏览的网页将会被记录在这个侧录页面上。	**Auditor > Web Recorder > Request** 

字段	说明	范例
Date	发送浏览网页要求的时间。	2006-6-19 14:40:24
Method	method 用以规范窗体被送出时，所采用的 HTTP method，默认值是 GET。POST 方法是将数据报装在 HTTP 标头内传送给 Web server；而 GET 方法则是将数据直接加在 URI 之后。使用 GET method 所能传递的数据有限（连同 URI 共 255 字符），在需要上传大量数据或档案时，必须使用 POST method。	get
Web Site	要浏览的网站。	us.js1.yimg.com
URI	Uniform Resource Identifiers 的缩写，资源标识符串，是用于在网络环境中识别文件、可供下载的档案、各式服务及电子邮箱等等的各式资源。	/us.yimg.com/lib/common/lsmfonts_20040826.css
Bytes	发送浏览要求的网页流量。	322
Src IP	发送浏览要求的来源端 IP 地址。	192.168.17.58
Src Port	发送浏览要求的来源端端口。	1811

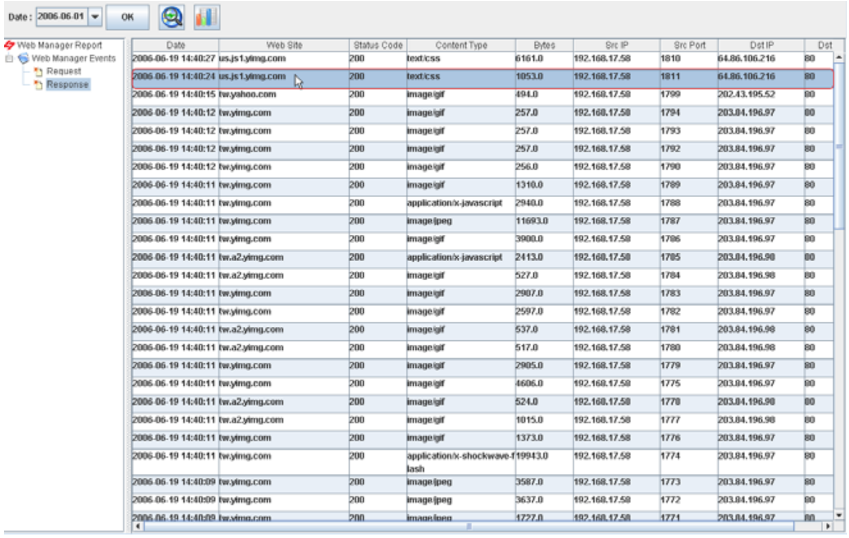
Dst IP	欲浏览的网站之 IP 地址。	64.86.106.216
Dst Port	欲浏览的网站之端口。	80

表格 23-2 网页侧录 - 浏览字段说明

步骤 2 回应的网页侧录

用来储存 request （要求） 生成的 response（响应）。响应的网页系依以上网页浏览要求发生时，对应的响应网页也会被侧录在这个页面上。

Auditor > Web Recorder > Response



字段	说明	范例
Date	响应浏览网页要求的时间。	2006-06-19 14:40:24
Web Site	要浏览的网站。	Us_js1.yimg.com
Status Code	状态代码值，表示网页浏览的成功或失败。	200
Content Type	网页内容型别标示。	Text/css
Bytes	响应浏览需求的网页流量。	1053.0
Src IP	浏览网页要求的来源端 IP 地址。	192.168.17.58
Src Port	浏览网页要求的来源端端口。	1811
Dst IP	欲浏览的网站之 IP 地址。	64.86.106.216
Dst Port	欲浏览的网站之端口。	80

表格 23-3 网页侧录 – 响应字段说明

第11部

系统维护

第24章 系统记录

24.1 需求

1. 网管人员希望知道过去所有系统执行状态，不希望有非法设定。
2. 网管人员每天必须核对系统操作记录，但是希望简化并缩减核对的程序。
3. 网管人员希望实时收到 alert （警告）与 critical（严重） 等级的事件记录，希望当系统有问题时，能实时提供解决之道。

24.2 目的

1. 网管人员希望知道过去所有系统的管理动作。
2. 网管人员希望每天收到 InstantScan 的记录报表。
3. 网管人员希望实时收到严重等级以上的系统记录。

24.3 方法

1. 透过系统记录的追踪，您可以检视管理动作的合法与否。
2. 透过 mailer 接收电子邮件。设定每天定时自动寄送记录文件给网管人员。
3. 在 mailer 上启用透过 e-mail 实时寄送系统记录。

24.4 步骤

24.4.1 系统记录

步骤 3 检视系统记录

您可以在 Functions > Reports > System Manager 页面上浏览所有的系统记录。系统记录依严重性分成 5 个等级。

Alert （警告）

Critical （严重）

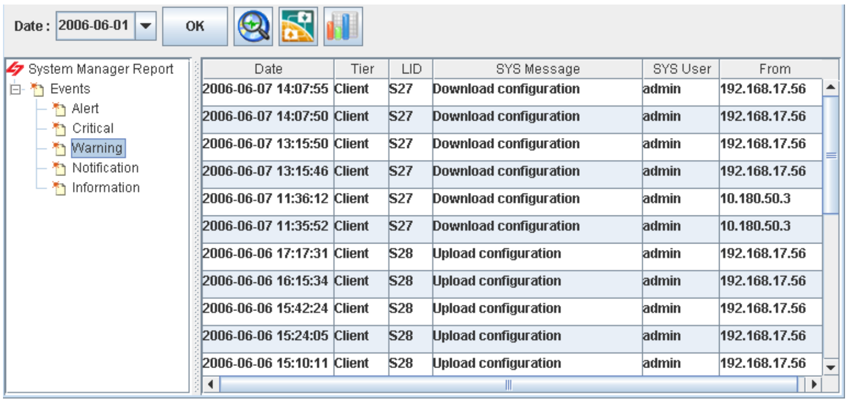
Warning （警示）

Notification （注意）

Information （信息）

系统记录详细信息请参考**错误！找不到参照来源。**。

Functions > Reports > System Manager



字段	说明
Date	系统事件记录产生的日期与时间。
Tier	产生系统记录的层级。因为 InstantScan 属于三层式体系结构，所以有 Device 层、Management Server 层，与 Client 层。
LID	系统记录的编号。
SYS Message	系统记录的操作说明，.

SYS User	登入并操作此 InstantScan 的使用者账号。
From	造成此系统事件的来源端。

表格 24-1 系统记录说明

24.4.2 设定接收系统记录的时间

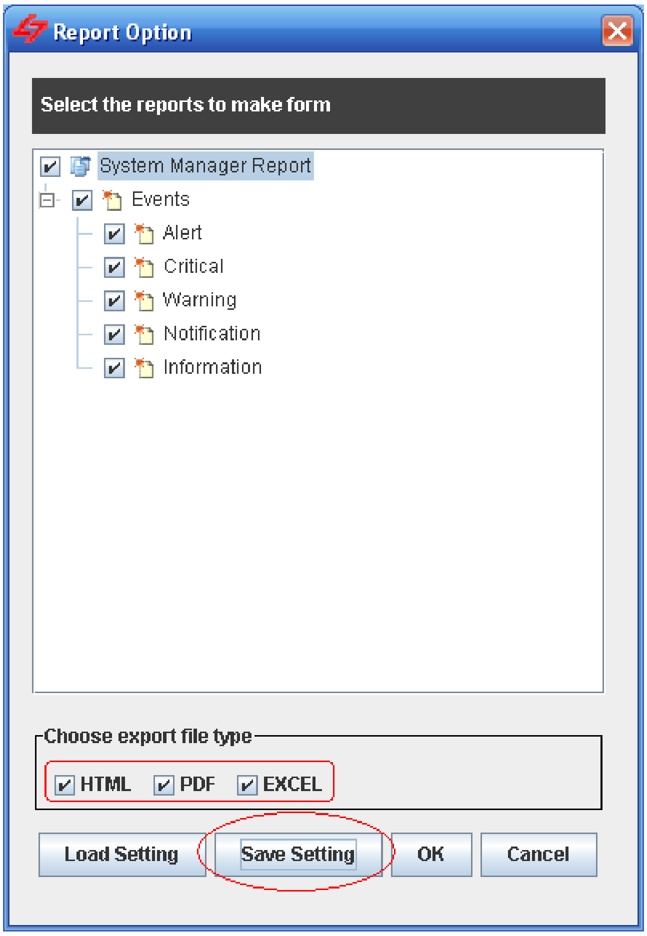
<table>
<tr>
<td>

步驟 1 设定系统记录的输出格式

在 Reports > System Manager 的页面上按图示。选择您有接收的报表类型，然后勾选输出报表的文件类型，最后点击 Save Settings。以后如果您升级韧体，只要点击 Load Settings，就可将之前的设定加载了。

</td>
<td>

Functions > Reports > System Manager > Export

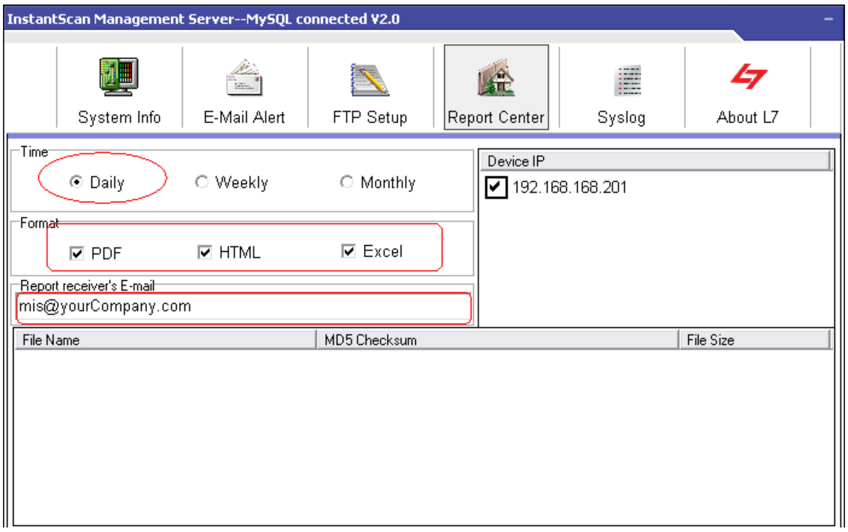


</td>
</tr>
</table>

步驟 2 设定接收系统记录的时间

在 mailer > Report Center 上选择希望接收系统记录报表的时间、报表格式及勾选要接收哪个装置上的系统记录。最后输入报表接收者的电子邮件信箱。

Mailer > Report Center



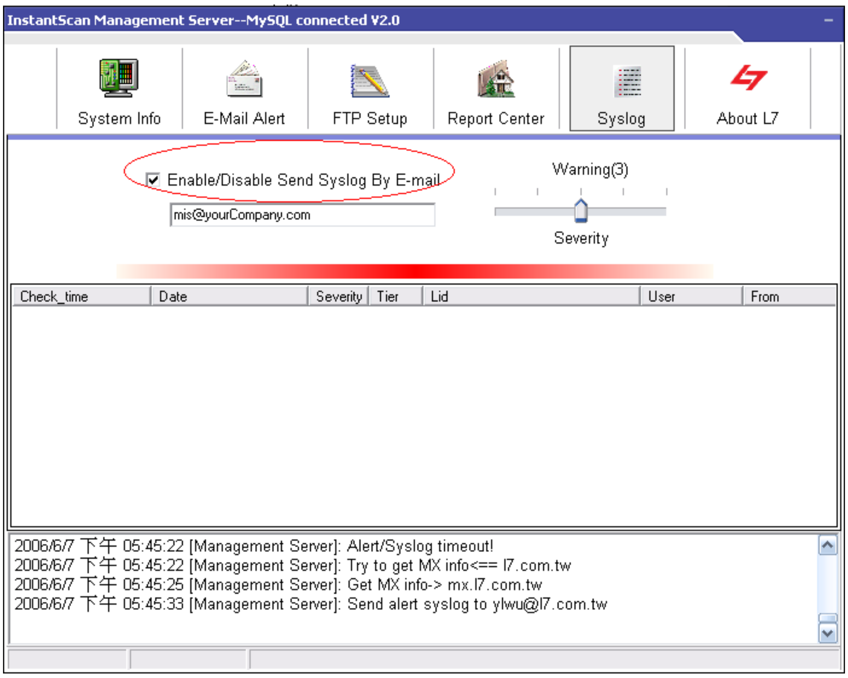
24.4.3 启用实时接收系统记录

步驟 1 启用透过电子邮件传送系统记录

勾选 Enable/Disable Send Syslog By Email，拉选您要实时接收系统记录的严重性，然后输入报表接收者的电子邮件账号。

设定完成后，每当有符合设定的事件记录产生，您便可实时接收电子邮件寄送的系统记录警告信件。

mailer > Syslog



第25章 系统维护

本章介绍系统维护。

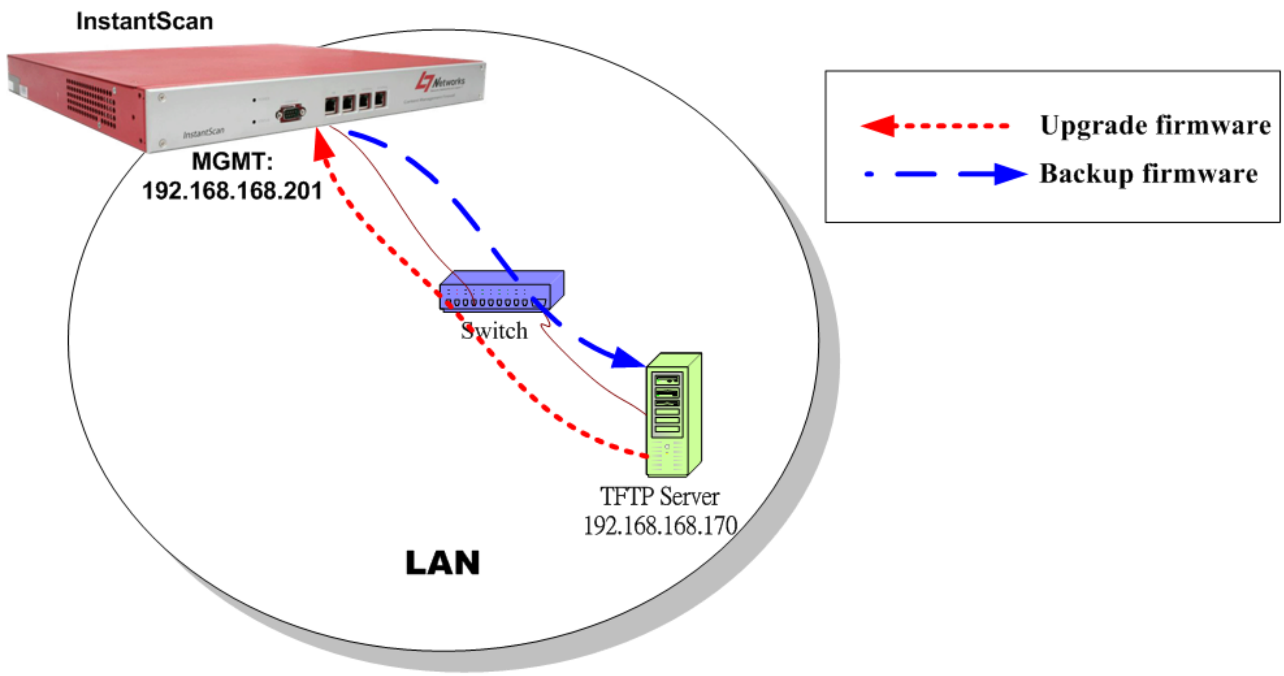
25.1 需求

1. InstantScan 让您可以随时更新韧体与数据库以符合当前的网络状态。新的功能、新的攻击、新的 URL 数据库，与新的病毒定义都需要不定时更新，所以本章介绍如果透过 TFTP 服务器与网页接口更新 InstantScan。

2. 当您忘记密码、韧体或配置文件损毁，您可以透过网页接口或是 console 接口将韧体恢复到出厂默认值。但当您忘记密码时，您只可以透过 console 接口，利用救援模式恢复出厂默认值。

3. 当您设定好 InstantScan 后，为避免因不明原因而造成配置文件损毁，所以您可以将现行的配置文件备份，以备不时之需。

25.2 透过 TFTP 服务器升级韧体



图表 25-1 从 TFTP 服务器处升级 / 备份韧体

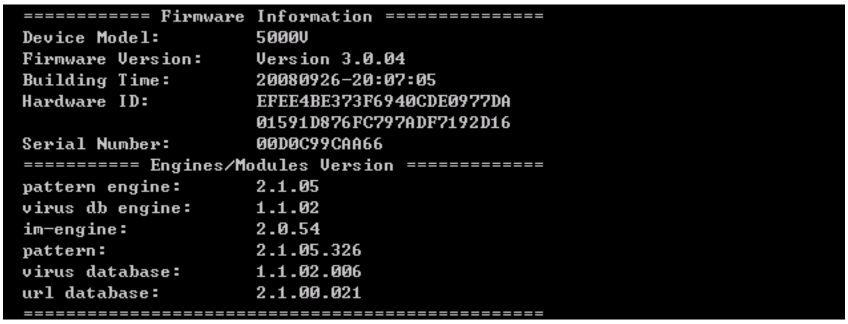
步骤 1 设定 TFTP 服务器 将 TFTP 服务器置于 C:\ 槽底下。将所有韧体扩展名为 bin 的档案也放在一起。将这台有安装 tftp 服务器的 PC 之 IP 地址设定与InstantScan LAN1 端的 IP 在同一个网段。登入 InstantScan console 界面。输入 ”en” 进入权限模式。	N/A

步驟 2 升级韧体

输入 ip tftp upgrade image <FILENAME> 192.168.168.170。完成后，InstantScan 将会重开机。相关 CLI 指令，请参考附錄 A 说明。

步驟 3 检查更新后的韧体设定

待重开机完成，请用sys ver检查所有相关设定是否正确。

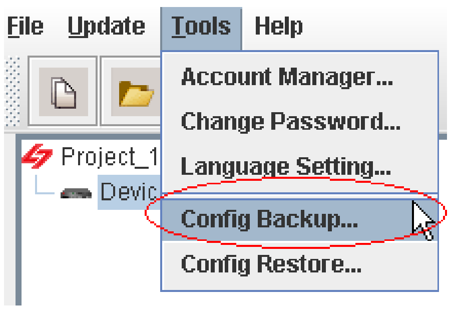


25.3 备份配置文件

步驟 1 备份配置文件

在工具栏上点击 **Tools**，然后点选 **Config Backup**。

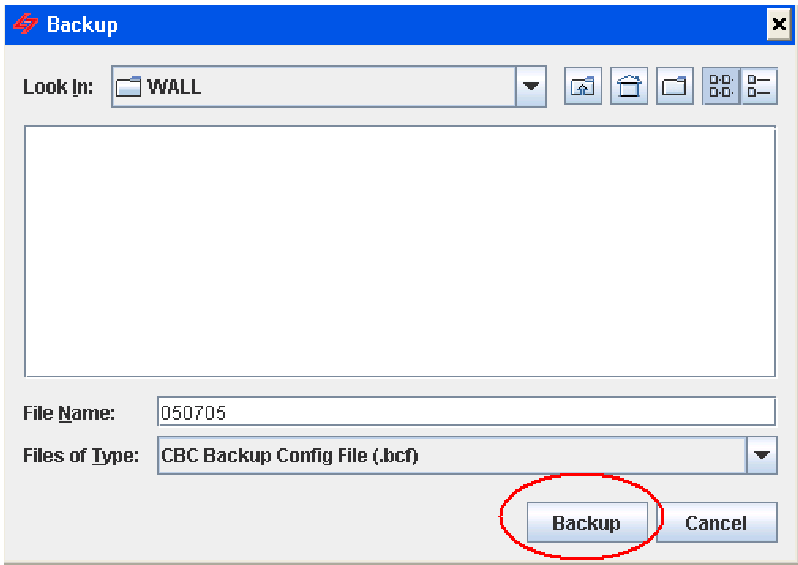
Tools > Config Backup



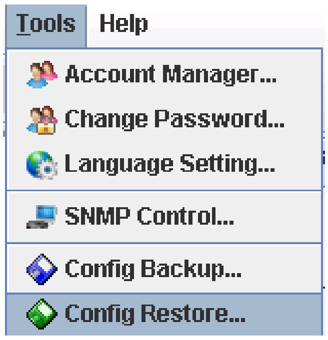
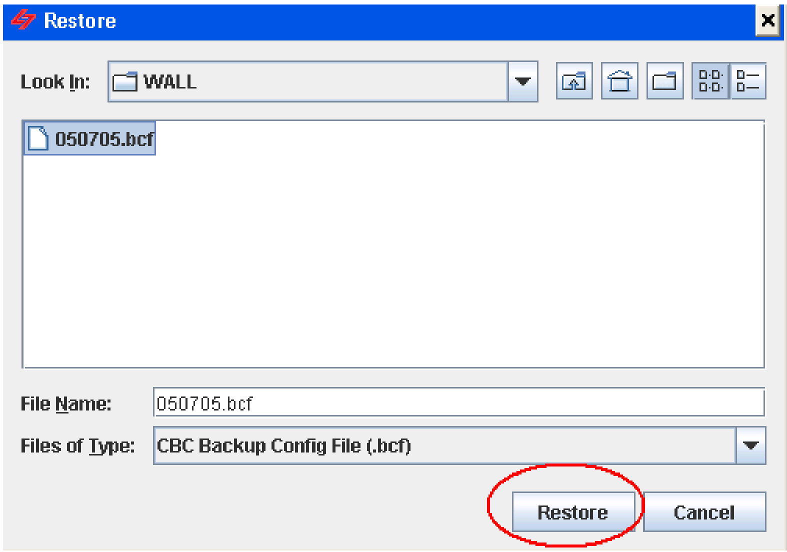
步驟 2 储存配置文件

请选择要将配置文件储存的文件夹，然后输入文件名。点击 **Backup** 完成设定。

Tools > Config Backup

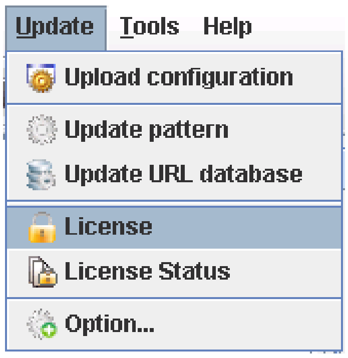


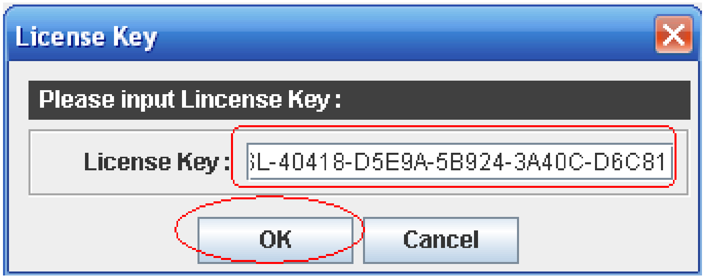
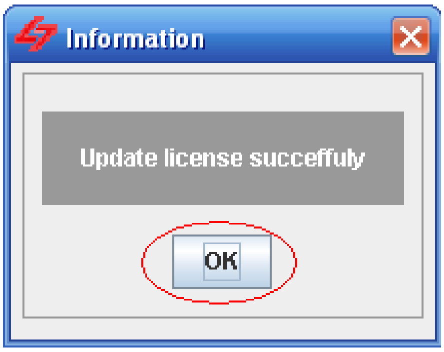
25.4 还原配置文件

<table>
<tr><td>步驟 1 还原配置文件
在工具栏上点击 Tools，然后点选 Config Restore。</td><td>Tools > Config Restore

</td></tr>
<tr><td>步驟 2 选择要还原的配置文件
请选择要还原的配置文件，然后点击 Restore 完成设定。</td><td>Tools > Config Restore

</td></tr>
</table>

25.5 启用选购的模块

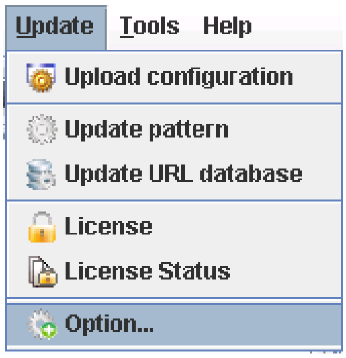
当您购买 InstantScan 时，只有标准的 Application Firewall 模块、Traffic Manager 模块、IM Manager 模块与 Object Manager 模块。如果您有选购 Web Manager，您必须透过用户接口上传 Web Manager 模块的 License Key 来启用它，否则您无法使用 Web Manager，且也无法在 UI 上面看到这个模块。

<table>
<tr><td>步驟 1 连上注册网页
在工具栏上的 update，点选 License。</td><td>Update > License

</td></tr>
</table>

步驟 2 输入 License Key 输入您所选购模块的授权码，然后点击 **OK** 继续。	**Update > License** 
步驟 3 上传授权码成功 当您上传授权码成功，将有如右图的窗口显示。	

25.6 升级 IM 引擎 / 应用程序行为 / 病毒数据库 / URL 数据库

25.6.1 自动升级 IM 引擎 / 应用程序行为 / 病毒数据库 / URL 数据库

步驟 1 自动更新设定 点击 **Option...** 。	**Update > Option…** 

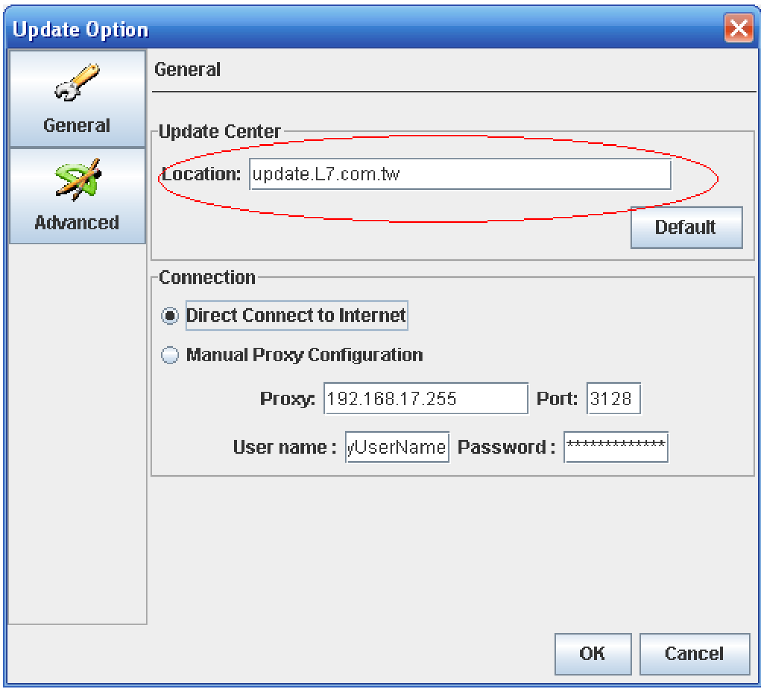
<table>
<tr>
<td>

步驟 2 输入更新中心数据

输入更新中心的地址，您亦可以点击 Default 按钮来获得默认的更新中心网址。然后选择联机方式，如果贵公司透过 proxy 服务器连上网络，请点选 Manual Proxy Configuration。然后输入 proxy 服务器的 IP 地址、服务器端口与您的用户名称 和密码。点击 Advanced 设定更新项目与排程。

</td>
<td>

Update > Option… > General



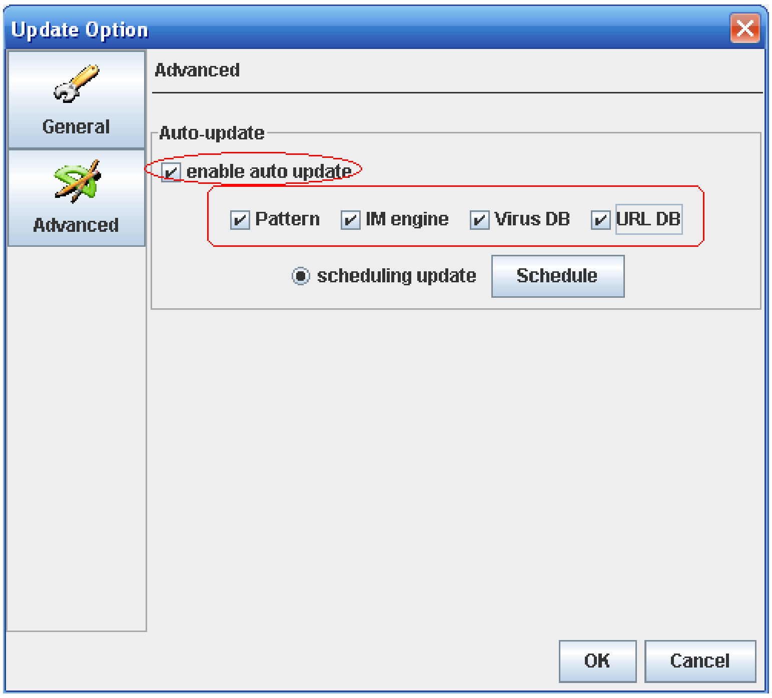
</td>
</tr>
<tr>
<td>

步驟 3 启用自动更新

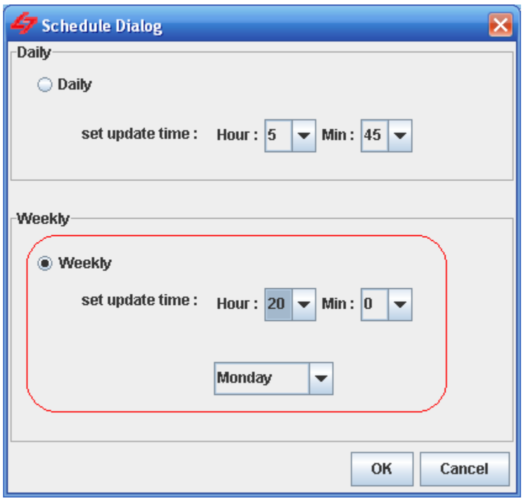
勾选 enable auto update，并勾选要自动更新的项目。点击 Schedule 设定更新排程。

</td>
<td>

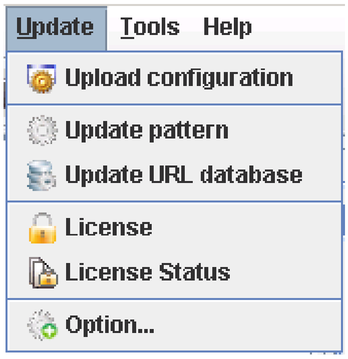
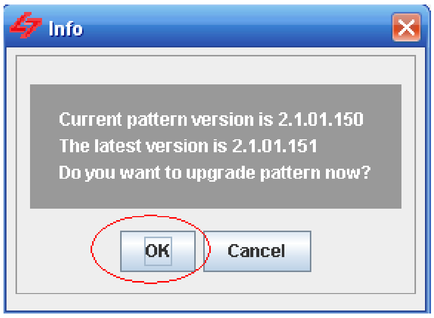
Update > Option… > Advanced



</td>
</tr>
</table>

步驟 4 设定更新排程 选择 Weekly，然后选择每周自动更新的时间与日期。点击 OK 完成设定。	**Update > Option… > Advanced > Schedule** 

25.6.2 手动升级应用程序行为

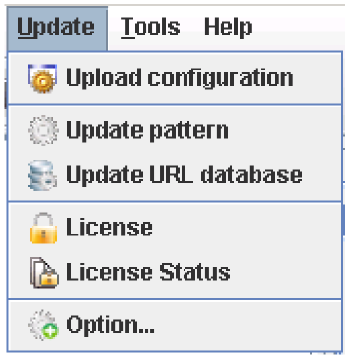
步驟 1 从 **UI** 上手动升级应用程序行为 点击 **Update pattern**。	**Update > Update pattern** 
步驟 2 更新应用程序行为 点击 OK 开始更新应用程序行为。	**Update > Update pattern** 

25.6.3 手动升级 URL 数据库

步驟 1 从 UI 上手动升级 URL 数据库

点击 **Update URL database**。

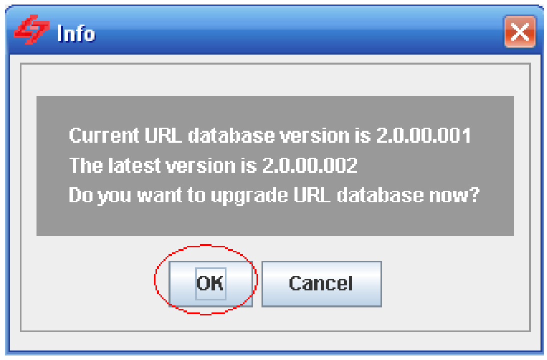
Update > Update URL database



步驟 2 更新 URL 数据库

如果您装置上的 url 数据库为最新版本，将出现右图的讯息。请点击 **OK** 结束更新的动作。

Update > Update URL database



25.6.4 在 CLI 标准模式下，恢复出厂默认值

步驟 3 恢复出厂默认值

在 CLI 模式下键入 **sys resetconf now**，按 Enter 后，系统将重新启动，所有设定将回复到出厂默认值。

25.6.5 在 CLI 救援模式下，回复出厂默认值

步驟 4 进入安全模式

在 5 秒的倒数计时内，按 ctrl+e，进入救援模式。在这个内核模式中，您可以利用 tftp 指令来安装韧体或者将配置文件回复到出厂默认值，甚至您忘记密码也可以在这个模式下操作。

输入 sys resetconf now，系统将重新启动将配置文件回复到出厂默认值。

```
Press ctrl+e in 5 secs to start with emergency kernel.
Enter emergency mode.

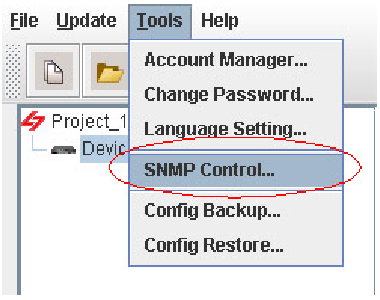

(Emergency Mode) login as "admin", no password
[EMERGENCY] login: admin
[EMERGENCY]> en
[EMERGENCY]#
  disable  Turn off privileged mode command
  exit     Exit command shell
  ip       Configure/Display IP related settings
  sys      Configure system parameters
[EMERGENCY]# sys resetconf now
Config reset to default.
System will reboot now
```

25.6.6 SNMP 控制设定

步骤 1 开启 SNMP 控制窗口

点选 Tool Bar 上面的 Tools 选项，就会跳出选单，点选 SNMP Control 选项之后，就会跳出 SNMP 的控制接口。

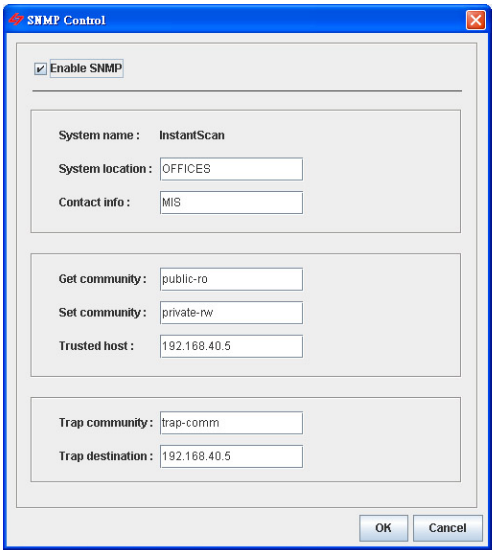
Tools > SNMP Control



步骤 2 设定 SNMP 控管

只要在接口上设定好 SNMP 各项参数，您就可以透过 SNMP 管理员远程监控 InstantScan 的系统状态、网络状态等。

Tools > SNMP Control



字段	说明	范例
启用 SNMP	启用 SNMP 远程监控。	启用
系统名称	InstantScan 装置名称。	WALL-1.yourCompany.com
系统位置	InstantScan 安装的位置。	Office
联系人信息	控管 InstantScan 的网管人员。	mis
Get community	透过社群可以获得 SNMP 的信息。这里的 get community 类似密码，用来做身份验证用。	public-ro
Set Community	透过社群可以获得 SNMP 的信息。这里的 set community 类似密码，用来做身分验证。	private-rw
信赖的主机	可以透过 InstantScan 获得或设定社群的 IP 地址。	192.168.1.5
Trap community	传送 SNMP trap 的社群。	trap-comm
Trap destination	透过 InstantScan 传送 SNMP trap 的 IP 地址。	192.168.1.5

附录

附錄 A
指令行接口（CLI）

您可以利用 web 接口（http/https）来设定 InstantScan，除此之外，当遇到紧急时刻，您亦可利用 console/ssh/telnet 远程联机方式来更改或查询设定。CLI 指令是非常有用的工具，它可以让您设定或更改所有接口的 IP 地址、将配置文件重设成出厂默认值或者是重开机。我们将所有 CLI 指令整理成以下表格，以供您参考。

A.1 CLI 指令列表 - 标准模式

当您透过 console/telnet/SSH 连上 InstantScan，必须使用 CLI 指令来设定 InstantScan。您可依据以下表格所描述的指令来完成 InstantScan 的设定。

非权限模式 Non-privileged mode

主要指令	次要指令	范例	指令说明
?		?	显示所有指令主选单
enable (en)		enable	开启权限模式指令
exit (ex)		exit	离开 CLI 界面
ip			设定相关 IP 参数
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	status (st)	sys status	显示系统与网络状态
	version (ver)	sys version	显示 InstantScan 韧体版本信息

表格 A-1 标准模式下的非权限模式

⚠ **注意：**如果您不晓得某个指令的参数，您可以在指令后空一格打问号” ?” 例如：“ip ?”。所有ip底下可能的参数就会显示出来。。

权限模式 **Privileged mode**

主要指令	次要指令	范例	指令说明
?		?	显示所有指令的主选单
disable (dis)		disable	关闭权限模式
exit (ex)		exit	离开 CLI 界面
ip			设定相关 IP 参数
	ifset	ip ifset INTF1	显示或变更网络接口设定
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	set	ip set	设定 InstantScan 相关 IP 地址
	show	ip show	显示所有网络设定
	tftp (upgrade)	ip tftp upgrade image <FILENAME> 192.168.168.170.	从 tftp 服务器处升级韧体
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	date	sys date	显示/设定目前系统时间
	halt	sys halt now	关机
	highavail	sys highavail set	High-Availability 相关参数设定
	module	sys module	更新/还原系统模块设定
	password	sys password	变更管理员密码
	reboot	sys reboot now	重开机
	resetconf	sys resetconf now	重设系统配置文件成出厂默认值
	sessionlog	sys ressionlog on	Session 记录的设定
	showmac	sys showmac	显示网络卡的 MAC 地址
	status (st)	sys status	显示系统状态
	tcpdump	sys tcpdump management	倾印 (dump) 流经的封包
	uptime	sys uptime	显示 InstantScan 正常运作的时间
	version (ver)	sys version	显示 InstantScan 韧体版本

表格 A-2 标准模式下的权限模式

完整的 sys module 与 ip tftp upgrade 指令，请参阅下表。

前缀指令	第二指令	第三指令	字尾指令	范例	指令说明
sys	module	flushstate	--	sys module flushstate	手动清除系统内闲置不用的联机
		query	--	sys module query	询问模块版本
		restore	all	sys module restore all	复原系统应用程序行

					为/特征码/病毒数据库
			av	sys module restore av	复原系统病毒和蠕虫数据库
			pattern	sys module restore pattern	复原系统应用程序行为
			signature	sys module restore signature	复原系统特征码
		setting	set	sys module setting set	更改更新服务器设定
			show	sys module setting show	显示更新服务器设定
		update	all	sys module update all	更新系统应用程序行为/特征码/病毒数据库
			av	sys module update av	更新系统病毒和蠕虫数据库
			pattern	sys module update pattern	更新系统应用程序行为
			signature	sys module update signature	更新系统特征码
ip tftp	upgrade	firmware	FILENAME tftp server IP address	ip tftp upgrade firmware <FILENAME> 192.168.168.170	从 tftp 服务器处升级韧体
		image	FILENAME tftp server IP address	ip tftp upgrade image <FILENAME> 192.168.168.170	从 tftp 服务器处升级 image 檔
		module	FILENAME tftp server IP address	ip tftp upgrade module <FILENAME> 192.168.168.170	从 tftp 服务器处升级系统模块

表格 A-3 Sys module 与 IP tftp 指令说明

⚠ **注意，IP TFTP upgrade字尾指令意义如下：**

WORD： tftp 服务器IP地址。

FILENAME： 升级配置文件或韧体的image文件名。

完整 sys sessionlog 指令，请参阅下表。

前缀指令	第二指令	第三指令	字尾指令	范例	指令说明
sys	Sessionlog	Off	--	sys sessionlog off	关闭系统记录
		On	--	sys sessionlog on	启用系统记录
		Status	--	sys sessionlog status	系统记录状态

表格 A-5 sys tcpdump 指令说明

完整 sys tcpdump 指令，请参阅下表。

前缀指令	第二指令	第三指令	字尾指令	范例	指令说明
sys	tcpdump	External	dump	sys tcpdump external dump	倾印流经 external 端的封包
			interactive	sys tcpdump external interactive	依交谈模式列举流经 external 端的封包
		Internal	dump	sys tcpdump internal dump	倾印流经 internal 端的封包
			interactive	sys tcpdump internal interactive	依交谈模式列举流经 internal 端的封包
		Management	dump	sys tcpdump management dump	倾印流经 management 端的封包
			interactive	sys tcpdump management interactive	依交谈模式列举流经 management 端的封包

表格 A-6 sys tcpdump 指令说明

A.2 CLI 指令列表 - 救援模式

如果原始韧体因某些意外而损毁，您需要利用救援模式将韧体回复到出厂默认值。将 InstantScan 重新启动后，在 5 秒钟的倒数程序内按 <ctrl> + e 键，请输入 admin 后进入救援模式。

非权限模式 Non-privileged mode

主要指令	次要指令	范例	指令说明
?		?	显示所有指令主选单
enable (en)		Enable	开启权限模式指令
exit (ex)		Exit	离开 CLI 界面
ip			设定相关 IP 参数
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	date	sys date	显示目前系统时间

表格 A-7 救援模式之非权限模式

权限模式 Privileged mode

主要指令	次要指令	范例	指令说明
?		?	显示所有指令主选单
disable (dis)		Disable	关闭权限模式
exit (ex)		Exit	离开 CLI 界面
ip			设定相关 IP 参数
	ping	ip ping 202.11.22.33	发送 ICMP 响应需求讯息

	set	ip set	设定 device 的 IP 地址
	show	ip show	显示所有网络设定
	tftp (upgrade)	ip tftp upgrade image <FILENAME> 192.168.168.170.	从 tftp 服务器处升级韧体 (相关设定与标准模式同)
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所经过的路径
sys			设定系统参数
	date	sys date	显示目前系统时间
	halt	sys halt now	关机
	reboot	sys reboot now	重开机
	resetconf	sys resetconf now	重设系统配置文件成出厂默认值
	resetpasswd	sys resetpasswd	变更管理员密码
	showmac	sys showmac	显示网络卡的 MAC 地址

表格 A-8 救援模式之权限模式

附錄 B
疑难解答

1. 安装 InstantScan 后为什么 MSN 或 Yahoo 都无法登入？

答：您可能碰到以下几种情况：

1-1 启动 IM Manager 功能后 User 无法登入 MSN

A. 先到 Report 中的 Application Firewall 查看 log 状况，是否被 IS 所阻挡？为何被挡？

B. 如果客户端的 MSN 无法登入是因为走 port 80，而我们只允许客户端走正常联机的 1863。请在客户端的 PC 上，把 MSN 中的进阶选项 TCP 打勾，取消勾选其他如 SOCKS、SOCKS 5、HTTP Proxy 选项。

C. 到防火墙端开 1 条规则 ※＝＞ LAN TO WAN Service：1863 Allow

1-2 启动 IM Manager 功能后 User 无法登入 Yahoo

A. 先到 Report 中的 Application Firewall 查看 log 状况，是否被 IS 所阻挡？为何被挡？

B. 如果客户端的 Yahoo 无法登入是因为走端口 80，而我们只允许客户端走正常联机的 5050。请在客户端的 PC 上，把 Yahoo 中的网络联机设定选择第一项 不需使用代理服务器，这时请勿选择其他选项。

C. 到防火墙端开 1 条规则 ＝＞LAN TO WAN Service：5050 Allow。

2. 如何知道目前设备的网络处理效能？

答：进入 Console 模式下，输入指令 sys status，可了解本装置的 CPU Loading、Concurrent Sessions 等等。

3. 如果我设定 Auto update pattern，那我如何得知目前最新 pattern 有哪些变动？

答：您有两个方法可以查询 pattern 变动情况：

3-1 在管理接口点选 Update ＞ Support list ，系统会自动开启 IE 浏览器告知您目前使用的 pattern 版本与其所支持的通讯协议。

3-2 请上利基网络网页 www.L7-Networks.com 点选 **网络安全 > 发行须知** 寻找最新版本的 pattern 内容，并点选内容最后附加的 Support List 链接，即可看到支持清单页面。

4. 最新版本的 Pattern 或 URL database 要怎样更新呢？

答：

4-1 在管理接口的工具栏上点选您要更新的项目，例如 Update > Update Pattern/Database。

4-2 在 console 模式中输入 sys module update all 或逐项更新 (例如 sys module update pattern)。在此之前，请先确认您的对外网络是畅通的。

5. 如何更新韧体呢？

答：首先请先接洽您购买本装置的经销商，向其取得最新韧体，然后在 Console 模式下输入指令 ip tftp upgrade image <文件名> （例如：ip tftp upgrade image filename.bin 192.168.1.10）。至于怎么设定 tftp 服务器与如何从 tftp 服务器升级韧体，请参考本手册章节**錯誤! 找不到參照來源。**。

6. 管理服务器为什么都收不到记录？

答：请依下列步骤检查您的设定：

6-1 请确认在 console 模式中已经设定好本装置对应的管理服务器 IP 地址了。

6-2 请确认管理服务器是否有安装个人防火墙。

6-3 如有启动防火墙，请于防火墙设定中开启三个让管理服务器与本装置间沟通用的端口（514、1080 与 3306）。

6-4 如果上述 3 个步骤都排除后，最后请确认在服务选项中的 LogServer 之服务是否已经启动了。

7. 为什么我在 Console 下都看不到画面？

答：

7-1 请确认终端机选项中，每秒传输位是否选择 115200。超级终端机上的设定值为（8 数据位、1 停止位、无同位检查、115200 每秒传输位）。

7-2 假如步骤 7-1 的设定皆已完整，还是无法进入 console 画面。那么请准备丨台 PC 或笔记本电脑与管理埠对接，然后 Ping 管理埠的 IP （出厂默认值为 192.168.1.1）查看 Request 是否有响应。

7-3 如果步骤 7-2 也 ping 不到管理埠之 IP，那么请直接将本装置连接到网络上，测试网络是否断线来测试硬件开机问题，再进一步确认硬件是否有损坏。

7-4 依上述步骤 3，将本装置连接到网络上，请依以下结果处理后续事宜：

A. 网络正常：请更换 Console 线。

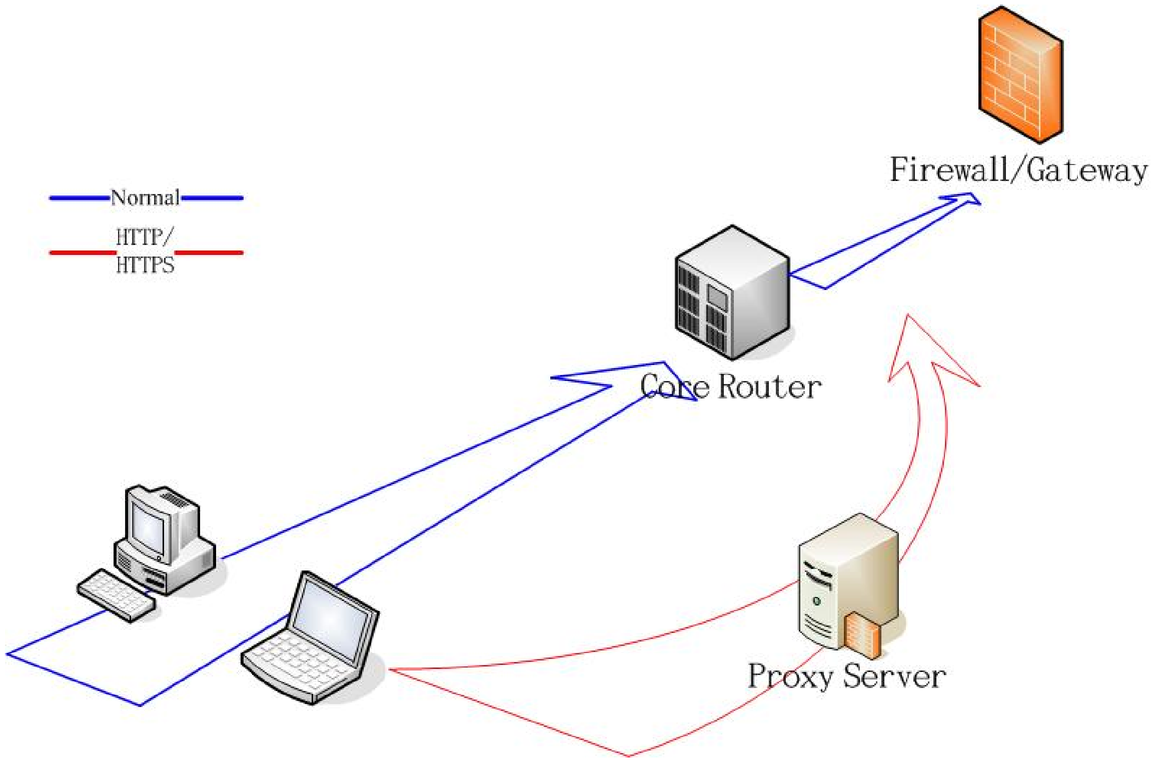
B. 网络断线：请用 RMA 方式联络原厂。

附錄 C
InstantScan 配置图暨相关设定调整建议

1. Cache Proxy
2. Cache Proxy + Limitations of Firewall
3. ISA Proxy Server
4. ISA Proxy Server（NAT）
5. Redirect to Web-Proxy

一、Cache Proxy

1. 图例



图表 B-1 普遍且没有限制的网络架构

2. 说明

除限制 HTTP/HTTPS 流量需透过 Proxy 代理，防火墙并无其他设定限定客户端上 IM/P2P 软件的使用。此为最常见的网络概况。此网络下，IM/P2P 不需额外调整设定即可自由地使用。

3. 配置暨设定

InstantScan 应配置在路由器与 Firewall/Gateway 之间。无需再另行调整其他设备上的设定。

4. 注意事项

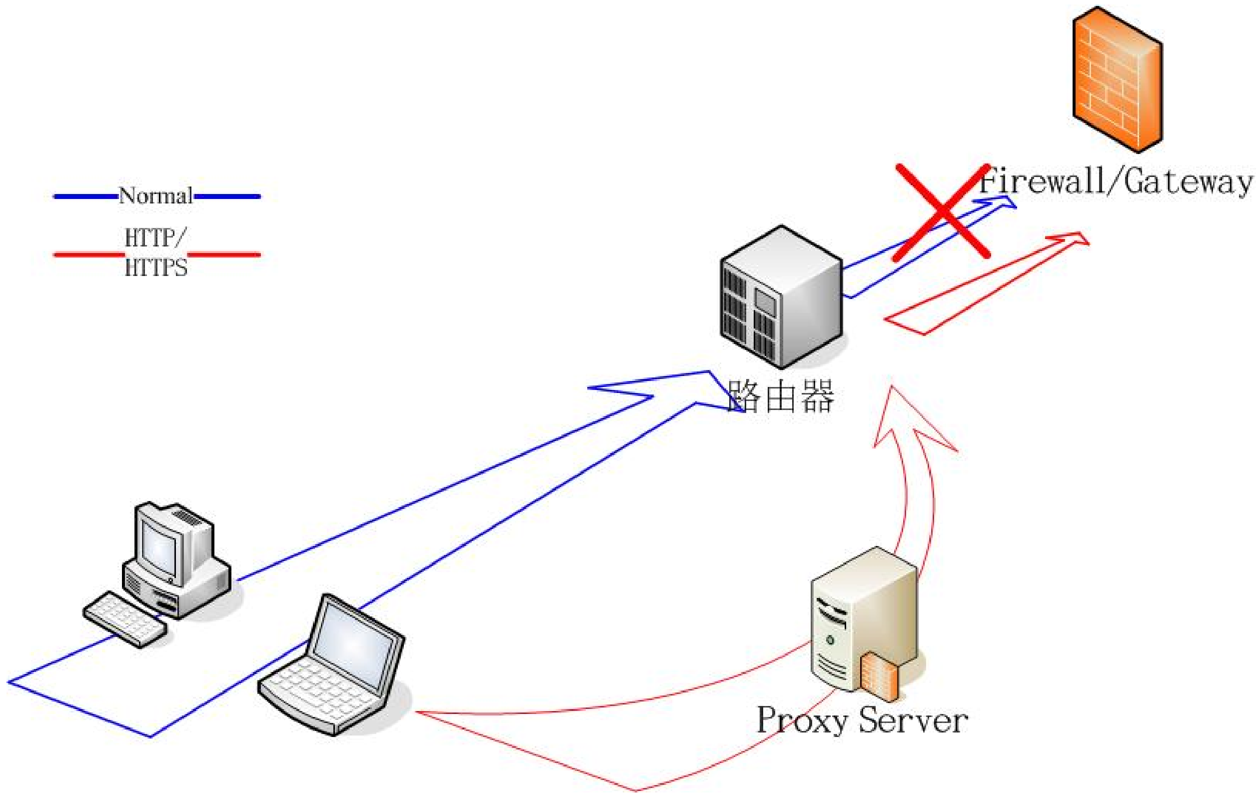
A. 如发现 Client 端在使用 MSN 时有无法登入的问题，可在 Proxy 设定 Deny URL http://gateway.messenger.hotmail.com/gateway/gateway.dll。此问题的发生在于 MSN 会尝试使用 IE 上的 HTTP

Proxy 设定，透过 port 80 与 MSN Server 联机，然而 InstantScan 在启动 IM 管理时，并不允许该种（非正规）联机方式，故产生 User 在不知情的状况下，因使用 port 80 之 MSN 联机被 InstantScan 阻挡而无法登入。

B. InstantScan 可于主干道上过滤所有流量，控管 IM 使用、阻挡 P2P 软件的联机及管制 P2P 带宽。

二、Cache Proxy + Limitations of Firewall

1. 图例



图表 B-2 有限度使用的网络架构图

2. 图例说明

Firewall/Gateway 限定只有 Server （HTTP/HTTPS Proxy、Mail） 的 IP 可自由通行，通常在这种环境下，主要目的为只让 User 使用 HTTP/HTTPS 联机，并透过 Proxy Server 管理/监控使用行为。

此种网络下，稍为进阶的 IM/P2P 软件用户，仍能透过设定软件中 HTTP（S）/SOCKS Proxy Server 的参数，经服务器代理而进行联机。一般第四层防火墙对此种方式完全无法管控。

3. 配置暨设定

InstantScan 应配置在路由器与 Firewall/Gateway 之间。设定方式如下：

A. 调整 Firewall 的政策，开放客户端可使用各项 IM 的标准端口 （MSN：1863、Yahoo：5050、ICQ：5190、AOL：5190），例：LAN （来源端） to WAN （目的端） 的端口 1863 方向之联机设定为允许通行。

B. 建议使用者取消各项 IM 上 Proxy 的设定，可减少无法联机的情形。

C. 建议在 Proxy 设定拒绝存取 URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止客户端在 MSN 尝试使用代理联机方式时，会等待较久时间才重新使用标准联机方式。

4. 注意事项

A. 原本可透过代理服务器进行联机的 IM/P2P 软件，因 InstantScan 能辨视出隐藏在 HTTP/SOCKS 的 IM/P2P 流量，故此类联机方式即被阻挡。

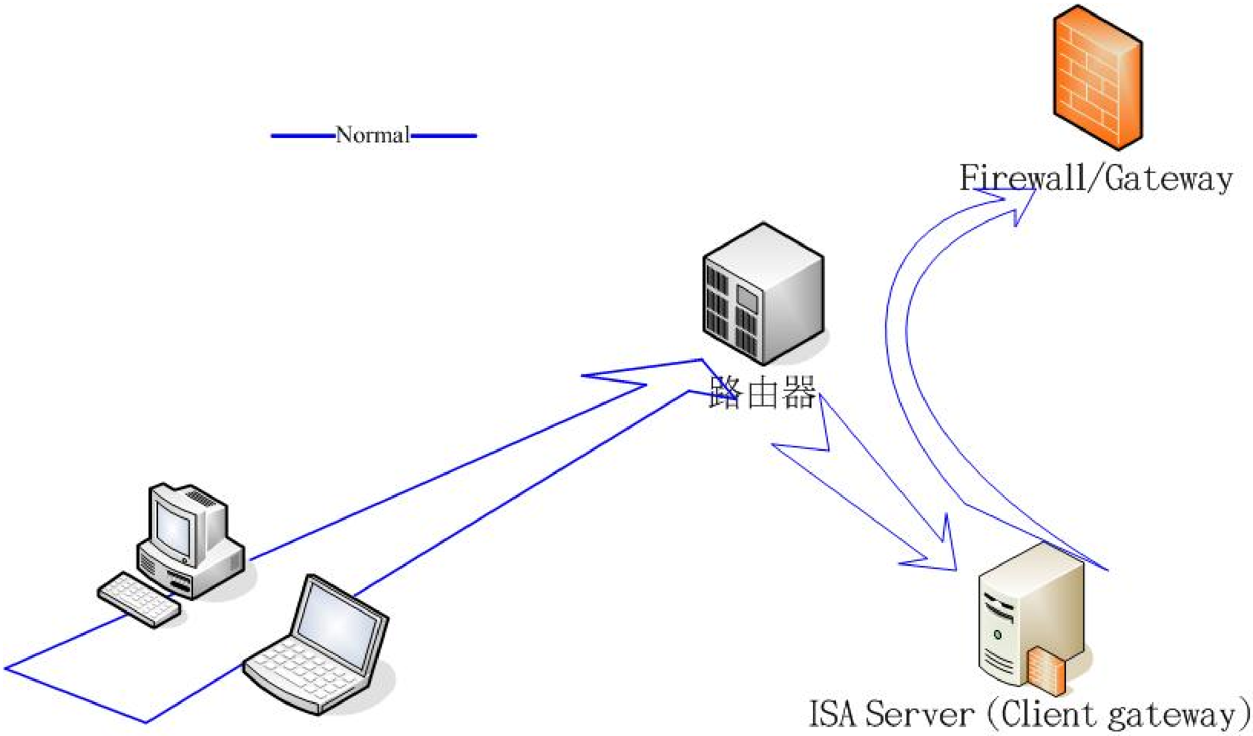
B. Firewall 开放客户端对外通讯，因设定是内部（LAN、trust）可存取外部（WAN、un-trust）服务器的服务（端口 1863、5050...等），由外部网络对内部网络（WAN to LAN）所发起的联机，仍处于被 Firewall 阻挡的保护下。

C. 开放各项 IM 的标准端口，InstantScan 可在这些通道内控管 IM。

D. 虽然 Firewall 内对外的适度开放，造成 P2P 软件可能会利用这些 IM 的端口进行联机，然而 InstantScan 的应用防火墙仍可以辨识出来并进行阻挡或管理带宽的工作。

三、ISA Proxy Server

1. 图例



图表 B-3 使用 ISA Server 做为 default gateway

2. 图例说明

在此种网络配置上，使用 Microsoft ISA Server 架设 HTTP 等代理服务器，并指定客户端的网络设定，将默认网关（default gateway）指向 ISA Server。ISA 除了会将 HTTP Proxy 等服务重新导向自己本身执行代理工作外，具备有 Firewall 与路由器能力的 ISA 会将其他的联机路由到出口的 Firewall/Gateway。

无论藉由 ISA Server 上的政策做为联机管制，亦或是由上一层的 Firewall 设定规则管制，就如同图例二的状况一样，无法防制进阶的 IM/P2P 软件用户透过 HTTP Proxy 的服务联机。

3. 配置暨设定

InstantScan 应配置在路由器与 Firewall/Gateway 之间。设定如下：

A. 调整 Firewall 或是 ISA Server 的政策，开放客户端可使用各项 IM 的标准端口（MSN：1863、Yahoo：5050、ICQ：5190、AOL：5190），例：LAN（来源端）to WAN（目的端）的端口 1863 方向之联机设定为允许通行。

B. 设定 ISA Server 需让各项 IM 的标准端口的联机可路由往出口网关。

C. 建议使用者取消各项 IM 上 Proxy 的设定，可减少无法联机的情形。

D. 建议在 Proxy 设定拒绝存取 URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止客户端在 MSN 尝试使用代理联机方式时，会等待较长久的时间才重新使用标准联机方式。

4. 注意事项

A. 原本可透过代理服务器进行联机的 IM/P2P 软件，因 InstantScan 能辨识出隐藏在 HTTP/SOCKS 的 IM/P2P 流量，故此类联机方式即被阻挡。

B. Firewall 开放客户端对外通讯，因设定是内部 （LAN、trust） 可存取外部 （WAN、un-trust）服务器的服务 （端口 1863、5050...等）， 由外部网络对内部网络 （WAN to LAN） 所发起的联机，仍处于被 Firewall 阻挡的保护下。

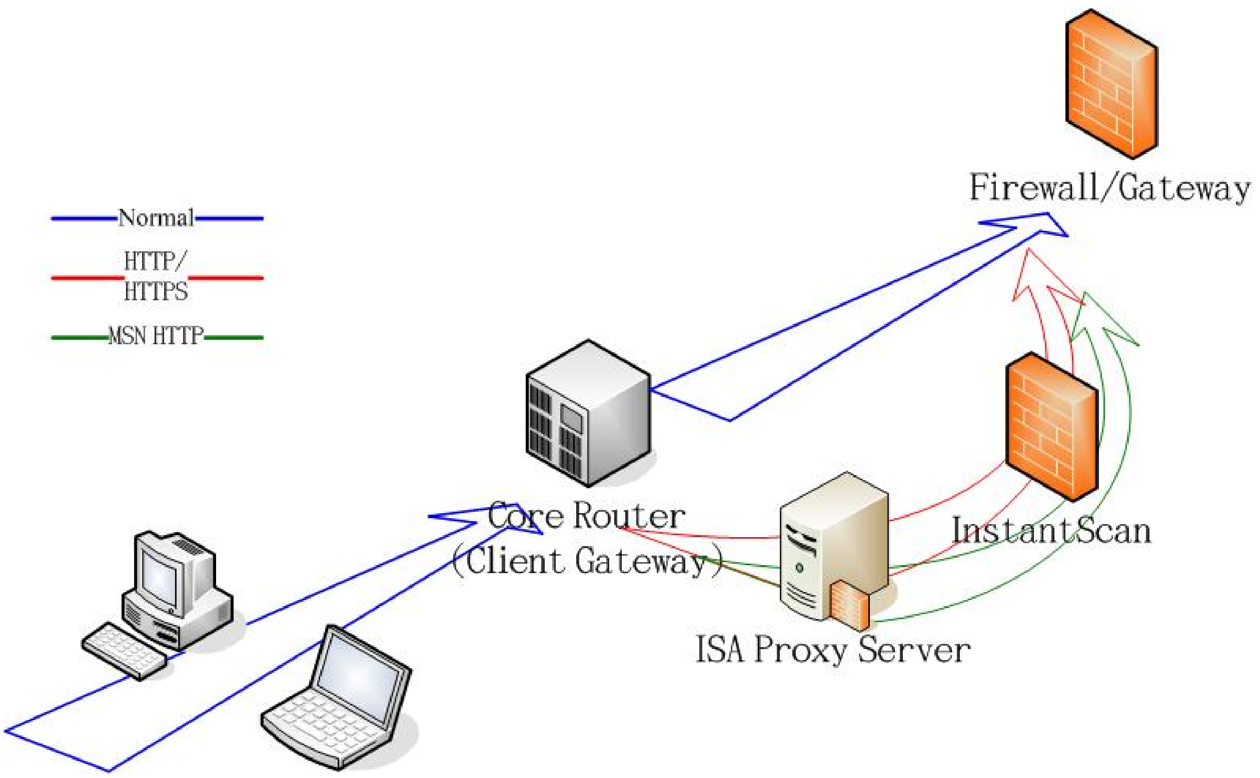
C. 因客户端的网关设定为 ISA Server，所以在 ISA Server 上必需确定经过 1863、5050、5190 及 5222 等端口的联机，会被重新路由往出口网关，联机才有办法建立。

D. 开放各项 IM 的标准端口，InstantScan 可在这些通道内控管 IM。

E. 虽然 Firewall 内对外的适度开放，造成 P2P 软件可能会利用这些 IM 的端口进行联机，然而仍可被 InstantScan 的应用防火墙辨识出来并进行阻挡或管理带宽的工作。

四、ISA Proxy Server（NAT）

1. 图例



图表 B-4 ISA Proxy Server 架构

2. 图例说明

使用 Microsoft ISA Server 架设 HTTP 等代理服务器，但并非将 gateway 指向 ISA Server，相对地仅教育使用者，将 IE 浏览器及 MSN 联机 HTTP Proxy 设定指到 ISA Server。

3. 配置暨设定

InstantScan 应配置在 ISA Server 往 Firewall/Gateway 的线路上。设定如下：

A. 在 Core Router 上设定政策，将各项 IM 的标准端口（MSN：1863、Yahoo：5050、ICQ：5190、AOL：5190、）导入 ISA Server。

B. 设定 ISA Server 为 NAT 模式，让一般流量或是各项 IM 的标准端口的联机可 NAT 往出口网关。

C. Firewall 设定允许来源地址为 ISA Server，且目的端端口为 1863、5050、5190、5222 通过。例：ISA 的 IP （来源端） to WAN （目的端） 的端口 1863 方向之联机设定为允许通过。

D. 建议使用者取消各项 IM 上 Proxy 的设定，可减少无法联机的情形。

E. 建议在 Proxy 设定拒绝存取 URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止客户端在 MSN 尝试使用代理联机方式时，会等待较长久的时间才重新使用标准联机方式。

4. 注意事项

A. InstantScan 所在的位置，只能管控 HTTP Proxy （IM-HTTP Proxy） 流量，故需做上述调整，让 IM 的正常联机，可通过 InstantScan 以进行 IM 管控。

B. 原本可透过代理服务器进行联机的 IM/P2P 软件，因 InstantScan 能辨视出隐藏在 HTTP/SOCKS 的 IM/P2P 流量，故此类联机方式即被阻挡。

C. Firewall 开放客户端对外通讯，因设定是内部 （LAN、trust）可 access 外部 （WAN、un-trust）服务器的服务 （端口 1863、5050...etc），由外部网络对内部网络 （WAN to LAN） 所发起的联机，仍处于被 Firewall 阻挡的保护下。

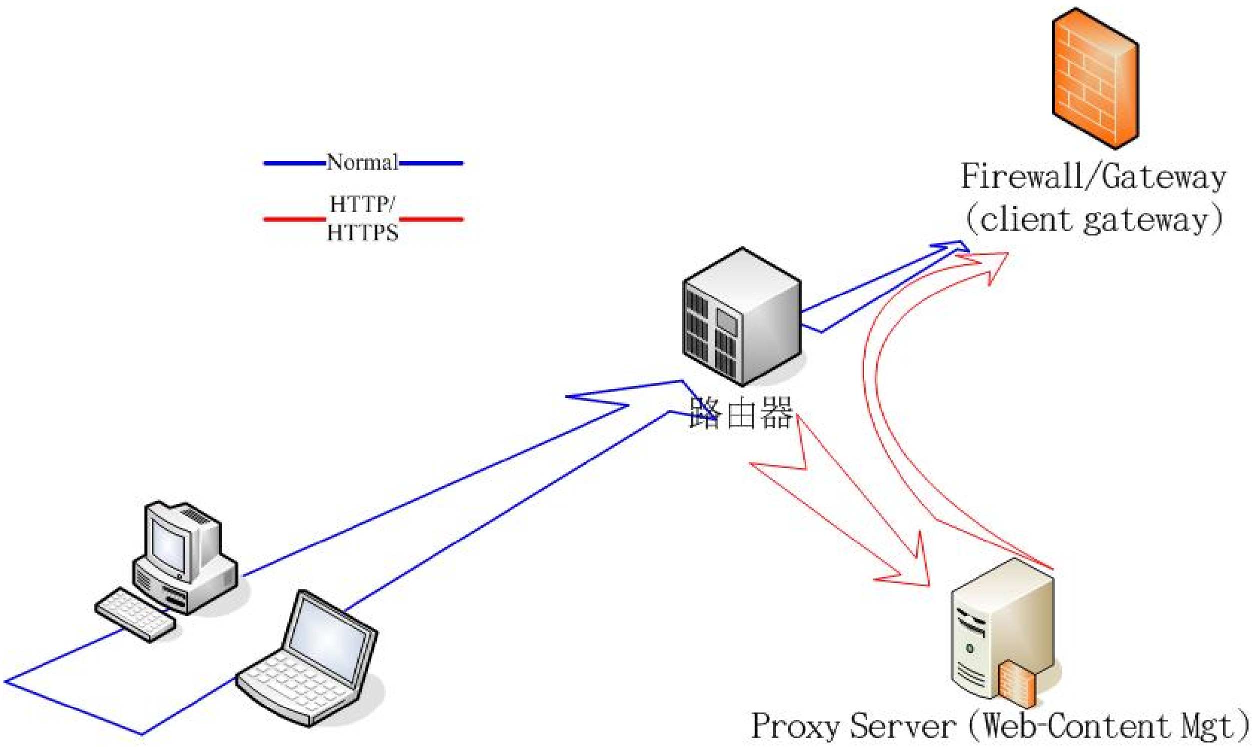
D. 由于原本的 IM 标准的联机方式，不会经过 InstantScan，故需借助 Core Router 将流量导入。

E. ISA Server 需使用 NAT 模式，目的是协助 MSN 可以建立标准联机。

F. Firewall 仅开放 ISA 可以使用开放的 80、443、1863 端口，故没有 P2P 软件可能会直接从主要线路 （不经过 InstantScan） 穿过的疑虑。

五、Redirect to Web-Proxy

1. 图例



图表 B-5 使用路由重导 HTTP 流量架构

2. 图例说明

联机藉由路由设备，过滤出通往 80、3128 等端口之联机；亦或借助有能力辨识 HTTP/HTTPS 联机之设备，将联机重新导向 Proxy Server、Web 管理服务器。此种方式的特点在于不需教导客户端调整任何设定即可达到 Web 行为的监控。

由于一般 Web 管理工具无法辨别 HTTP 联机中的内容，IM/P2P 透过 HTTP 模式联机时，便可藉助 Proxy 之便穿出防火墙；使用 HTTP 协议而发展出的 Tunnel 软件，也可建立联机，将内部网络曝露在不安全的环境下。

3. 配置暨设定

InstantScan 应配置在路由器与 Firewall/Gateway 之间。设定如下：

A. 调整 Firewall 的政策，开放 Client 可使用各项 IM 的标准端口（MSN：1863，Yahoo：5050，ICQ：5190，AOL：5190），例：LAN （来源端） to WAN （目的端） 的端口 1863 方向之联机设定为允许通过。

B. 建议在 Proxy 设定 Deny URL http://gateway.messenger.hotmail.com/gateway/gateway.dll 以防止 Client 在 MSN 尝试使用代理联机方式时，会等待较久时间才重新使用标准联机方式。

4. 注意事项

A. 原本可透过代理服务器进行联机的 IM/P2P 软件，因 InstantScan 能辨视出隐藏在 HTTP/SOCKS 的 IM/P2P 流量，故此类联机方式即被阻挡。

B. Firewall 开放客户端对外通讯，因设定是内部 （LAN、trust） 可存取外部 （WAN、un-trust）服务器的服务 （端口 1863、5050...等），由外部网络对内部网络 （WAN to LAN） 所发起的联机，仍处于被 Firewall 阻挡的保护下。

C. 开放各项 IM 的标准端口，InstantScan 可在这些通道内控管 IM。

D. 虽然 Firewall 内对外的适度开放，造成 P2P 软件可能会利用这些 IM 的端口进行联机，然而 InstantScan 的应用防火墙仍可以辨识出来并进行阻挡或管理带宽的工作。

附錄 D
系统记录语法

系统记录语法

InstantScan: time=2005-01-10 12:57:27; mod=SYS; sev=<1|2|3|4|5>; tier=<TIER>; lid=<LID>; msg=<Message>; by=<user|system>; from=<IP|console|system>;

严重等级	***Level name***
1	Alert （警告）
2	Critical （严重）
3	Warning （警示）
4	Notification （注意）
5	Information （信息）

TIER	***LID***	***Message***	***Severity***
Client tier=1	A01	Login success	Information
	A01	Login fail, miss password	Information
	A02	Change password	Information
	A04	A new user <user> has been added	Notification
	A05	User <user> has been deleted.	Notification
	A07	Login user <user> login failed due to invalid user name	Information
	S25	Backup configuration file by admin	Warning
	S26	Restore configuration file by admin	Warning
	S27	Download configuration	Warning
	S28	Upload configuration	Warning
Mgtsvr tier=2	L01	Database is full	Critical
	L02	Database is cleanup	Critical
	L03	Backup database to 192.168.17.130	Warning
	L04	Send report to user@yourCompany.com	Information
	L05	Restore database from 192.168.1.1	Warning
	L06	Send alert to user@yourCompany.com	Information
	M01	Change E-Mail Alert setting	Notification
	M02	Change FTP Backup setting	Notification
	M03	Change Report Center setting	Notification
	M04	Change Syslog setting	Notification
Device	A03	Login success	Information

tier=3z	A03	Login fail, miss password	Information
	A06	Change password	Information
	S01	Device Startup	Warning
	S02	Device Reboot	Critical
	S03	MGT set to192.168.17.114	Notification
	S04	Gateway IP set to 192.168.17.254	Notification
	S05	Primary DNS set to 10.1.1.1	Notification
	S06	Secondary DNS set to 168.95.1.1	Notification
	S07	Management server set to 192.168.17.112	Notification
	S08	System time updated to 2005-09-04 12:00:00	Notification
	S09	Factory reset to default settings	Warning
	S10	Firmware upgraded to version X.X.XX	Warning
	S10	Firmware upgrade has failed	Critical
	S11	Application Firewall pattern updated to version X.X.XX.XXX	Warning
	S11	Application Firewall pattern update has failed	Critical
	S12	IM signature updated to version X.X.XX.XXX	Warning
	S12	IM signature update has failed	Critical
	S13	AVDB updated to version X.X.XX.XXX	Warning
	S13	AVDB update has failed	Critical
	S14	Enable application firewall	Notification
	S14	Disable application firewall	Notification
	S15	Enable IM Manager	Notification
	S15	Disable IM Manager	Notification
	S16	Enable Traffic Manager	Notification
	S16	Disable Traffic Manager	Notification
	S17	Enable HA	Critical
	S17	Disable HA	Critical
	S18	HA mode changed to AA	Critical
	S18	HA mode changed to AS	Critical
	S19	HA type changed to master	Critical
	S19	HA type changed to slave	Critical
	S20	HA monitored node <node_name> failed	Warning
	S21	HA control changed to master	Alert
	S21	HA control changed to slave	Alert
	S22	HA Virtual IP Address: 192.168.17.100	Notification
	S23	HA In-Ping-Nodes: 192.168.17.111	Notification
	S24	HA Ex-Ping-Nodes: 192.168.17.254	Notificaiton

	S29	URLDB	
	S31	Application Firewall pattern updated to version X.X.XX.XXX	Warning
	S31	Application Firewall pattern update has failed(error code:XX)	Critical
	S32	reserved for future using	
	S33	AVDB updated to version X.X.XX.XXX	Warning
	S33	AVDB update has failed(error code:XX)	Critical
	S34	URLDB updated to version X.X.XX.XXX	Warning
	S34	URLDB update has failed(error code:XX)	Critical
	S35	IM engine updated to version X.X.XX	Warning
	S35	IM engine has failed(error code:XX)	Critical
	S36	Application Firewall engine updated to version X.X.XX	Warning
	S36	Application Firewall engine update has failed(error code:XX)	Critical
	S37	reserved for future using	
	S38	Antivirus database engine updated to version X.X.XX	Warning
	S38	Antivirus database engine update has failed(error code:XX)	Critical
	S39	URL database engine updated to version X.X.XX.XXX	Warning
	S39	URL database engine update has failed(error code:XX)	Critical
	S40	reserved for future using	
	S41	Application Firewall pattern restored to version X.X.XX.XXX	Warning
	S41	Application Firewall pattern restore has failed(error code:XX)	Critical
	S42	reserved for future using	
	S43	AVDB restored to version X.X.XX.XXX	Warning
	S43	AVDB restore has failed(error code:XX)	Critical
	S44	URLDB restored to version X.X.XX.XXX	Warning
	S44	URLDB restore has failed(error code:XX)	Critical
	S45	IM engine restored to version X.X.XX.XXX	Warning
	S45	IM engine restore has failed(error code:XX)	Critical
	S46	Application Firewall engine restored to version X.X.XX	Warning
	S46	Application Firewall engine restore has failed(error code:XX)	Critical
	S47	reserved for future using	
	S48	Antivirus database engine restored to version X.X.XX	Warning
	S48	Antivirus database engine restore has failed(error code:XX)	Critical
	S49	URL database engine restored to version X.X.XX	Warning
	S49	URL database engine restore has failed(error code:XX)	Critical
	S50	reserved for future using	
	S51	$SWID (Update Successfully. Update database and then respond a new SWID.)	

	S52	$SWID (Keep old license. Don't need to update database and then respond the old SWID.)	
	S53	Request is rejected	
	S54	Invalid HWID	
	S55	This device is not registered	
	S56	This license is invalid	
	S57	This license has been registered	
	S58	This license cannot be used on this device	
	S59	Can not connect to database	
	S60	No such device	
	S61	Can not connect to device	
	S62	Unable to clear database table	
	S63	Filter List error	
	S64	Post parameters error	
	S65	Post value is invalid	
	S66	Invalid software ID	
	S67	Execute SQL command fail	
	S68	No version obtained	
	S69	No such database	
	S70	Backup database fail	
	S71	Restore database fail	
	S72	Unmatched pattern version	
	S73	Software ID was reset to trial version	
	S74	Invalid checksum	
	S75	Can not find backup SQL scheme	
	S76	Enable Web Manager	Notification
	S76	Disable Web Manager	Notification

表格 D-1 系统记录格式说明

附錄 E
词汇集

DDoS （分段式阻断服务，Distributed Denial-of-Service ）

DDoS 是 DoS 的一种变形，因为它是透过网络分散来源的技巧，所以将之称作分散 式 DoS（Distributed DoS，简称 DDoS）攻击。

DoS （Denial of Service ）

DoS 是一种入侵程序，可以让计算机无法直执行某些动作，或者无故当机。与一般黑客入侵不同的是，DoS 攻击并不会让计算机内部数据遭到窃取或窜改，而是以瘫痪主机为目的。

FTP （文件传输协定 File Transfer Protocol）

FTP 是在传输控制协议 （TCP/IP ） 网络使用的一种档案通讯协议，定义如何将一个计算机系统，连接现有的网络（Network） ，以便存取网络上的系统资源。其主要工作是提供档案非录清单，负责文件传输与转换工作。

H.323

H.323 规范是在 1996 年经国际电信联盟认定，可以解决多媒体传输所要求的实时性与连续性问题。其主要内容是在定义分封交换网络上终端机之间的压缩和解压缩标准、通话程序及媒体传输等协议，同时也定义了在分封交换网络上的终端如何与传统的电话网络互相通话的机制。H.323 界定语音及视讯的压缩 / 解压缩设备，双方沟通的设定与控制。在语音方面，它支持多种标准，其中以 G.711 为主；至于视讯方面，H.323 则支援 H.261 与 H.263 两种主要的视频压缩 / 解压缩标准。

IM （实时通讯，Instant Messaging）

实时通讯是一种聊天应用，透过因特网实时地与他方用户传送文字简讯，现在更可以传送档案、语音、视讯或玩网络游戏等。

IPS （异常侦测，Anomaly-Based IPS）

异常侦测则是对用户或网络流量先建立一个「正常」的行为，再对通过的封包去做比对，假如超过正常行为的门坎值就是视为异常。此种做法的优点是可以侦测未知型态的入侵，但是误判率会表较高。

IP Spoofing （IP 地址欺伪）

这是一种攻击者得知主机地址之后，利用外部封包攻击主机的方法，由于封包 （Packet） 的来源地址和内部封包一样，因此主机 （Host） 会认为这是来自内部的封包，因而允许进行链结 （Link） ，这种攻击方法也会被内部破坏者使用。

LDAP （Lightweight Directory Access Protocol）

LDAP 是 Lightweight Directory Access Protocol 的简称，是目前最流行的目录服务 （Directory Service, DS） 存取协定。

License Key （授权码）

InstantScan 由多个模块组成，某些模块必须购买授权码并于开机时输入此授权码才可以启用该服务。

P2P （点对点，Peer-To-Peer）

这是一种传输模式，以点对点的方式传输讯息，例如曾经疯狂流行过的 Napster （Napster），就是以点对点的方式传输，使用者在对方提供的文件服务器上直接上传或下载 （Download） 乐曲；P2P 架构要比主从架构 （Client/Server） 简单便宜，因为无须太多高深的技术就可以执行，不过当网络负担太重的啥喉，传输的状况就不会比主从架构理想。

Port

数据 （Data） 进入或出去的一个接连点。

Protocol （通讯协议）

一个议定主要的就是几个通信处理之间，要被交换的一些讯息格式和讯息内涵的一组协约或规则。让实施和使用更加方便，在一些复杂的网络 （Network） 中，高阶议定可以用一种分层的方式来使用一些低阶议定。

RADIUS （远程认证拨接使用者服务，Remote Authentication Dial-In User Service）

RADIUS 是被许多因特网服务供货商 （ISP ） 所使用的认证与记账系统。当你拨入 ISP 时，你必须输入你的用户名称和密码。这个信息被传送到 RADIUS 服务器 （Server） ，查看信息是否正确，并授权 ISP 系统的存取。虽然 RADIUS 不是一个公认的标准，但是它的规格是由因特网工程工作团队所维持。

RDP （远程桌面协议，Remote Desktop Protocol）

RDP 是 Windows 终端机服务器和客户端用来彼此通讯的通讯协议。 客户端会利用它将击键及鼠标点按信息传送到服务器，而服务器则会利用此协议将显示 信息传送给客户端。

Router （路由器）

路由器又称为路径器，用户在网络层上连接不同网络所用的硬件与软件，路由器与网桥 （Bridge） 的功能类似，借着将许多较小的网络链接在一起，以便有效扩充网络。路由器可以连接使用不同因特网通讯协议 （IP ） 和传输方法的局域网络 （LAN ） 。

RS-232

RS-232 为 EIA 标准，是装置间链接数据最普遍的方式。

Scan

Scan 可以是端口、IP 或弱点扫描。黑客扫端口来寻找入侵的目标。他们可能使用 TCP connect（） call、SYN 扫描（half-open scanning）、Nmap 等等。

Severity

入侵攻击的严重性被定义成最低到最严重 5 个等级，其对默认对应的动作视其严重性而定。

Signature

特征码是辨识恶意软件之独特的行为模式。

Smurf Attack

Smurf 攻击者将伪造来源的 ICMP echo request 封包送到 IP broadcast addresses，而来源地址设成被害者的地址，造成 broadcast 地址回传大量的 ICMP echo reply 封包给被害者，使被害者的网络拥塞甚至中断。

Spam （垃圾信件）

Spam 原是一种美国肉罐头的商标，随着因特网 （Internet） 的出现，而被用来指称垃圾电子邮件 （E-mail ） ，这类垃圾邮件内含许多使用者可能不想看的商业广告，并传送给大量的收件人。用于动词时，则是指将许多用户不想要的讯息（message（MESG）（MSG）） ，贴在相关的邮件或网页上。

Spoofing （欺伪）

指的是以未经过授权的身份，在网络 （Network） 上从事传输动作，通常是恶意的行为。

SSL （Secured Socket Layer）

SSL 是将公钥的加密技术加入合并到网景领航员 （Netscape Navigator） 的网络浏览器 （Browser ） 里面，还有网景公司商业用的服务器 （Server） 里，且目前大多数的网络 （Network） 服务器与浏览器也已经采用 SSL。SSL 的加密与解密过程当中，必须透过密码簿中的密钥才能将乱码完全解开，为了确保使用者拿到的密钥安全性与公正性，密钥必须透过具有公信力的服务器认证中心认证。

SYN Attack

此种攻击方式主要是利用 TCP 连结的 three way handshaking 的缺陷。在 TCP/IP 通讯协议中，传输双方 （A、B） 的连结方式是，A 会从特定端口送出一个 SYN 封包给 B 的特定端口，而此时 B 会响应一个 SYN-ACK 的封包给 A，如果顺利到达，A 会再回送一个 ACK 的封包给 B 作确认。在完成这些程序之后，A 与 B 便能确认彼此的连结，此时联机建立，双方能够沟通，并传送与收发数据。SYN 这类攻击让 TCP 协议无法完成三次握手协议;

TCP （传输控制协议 Transmission Control Protocol）

TCP/IP 是一组用来连接因特网 （Internet） 上主机 （Host） 的协议标准。TCP 相当于开放系统互连参考模型的第四层（运输层） 协议，而 IP 则相当于 OSI/RM 的第三层（网络层）协议。但 TCP/IP 通常是指一组完整的网络协议。

Teardrop

Teardrop attack 的目的不是要去偷取你计算机中的数据，而是要让用户的计算机当机无法继续使用。利用封包重组时的弱点，当数据经由网络传送，IP 封包经常会被切割成许多小片段。每个小片段和原来封包的结构大致都相同，除了一些记载位移的信息。而 Teardrop 则创造出一些 IP 片段，这些片段包含重迭的位移值。当这些片段到达目的地而被重组时，可能就会造成一些系统当机。当它检查到后面片段的资料长度大于重迭的资料片段时，重迭部份将会被略过，但是后面的片段的数据长度小于重迭的数据片段时，使得数据片段长度太小，当接收到传来的封包时，只会去检查是否太长，是否应该舍弃重迭多余的部分，但却不会去检查是否太短而造成了错误.

Telnet

终端机 （terminal（T）（TERM）（TML）） 仿真程序是远程登录的因特网通讯协议 （IP ），使计算机用户可与服务器 （Server） 做交互式的连结，并存取 （Access） 远程网站。

Terminal Emulator （终端机仿真器）

容许在个人计算机和主计算机或装置间做同步数据传送，而数据则以主机可接受的格式来交换。。

TFTP （简单文件传输协议 Trivial File Transfer Protocol）

TFTP 是 TCP/IP Protocol 中的一员，和 FTP 一样是传输档案用，但是 FTP 是使用 TCP，但是 TFTP 是使用 UDP 来传输，使用 UDP 是不作传输数据正确性的验证，所以实际的文件传输是不会使用到 TFTP，然而若您是经常使用网络设备如 Terminal Server、Router 或是 SNMP Hub 的话，那您便可能需要使用 TFTP 来 Upgrade 网络设备的 Firmware 或 Software。

Transparent Mode （透通模式）

产品的复杂作业情形已被隐藏起来，用户使用产品时一点都不会觉得有何困难，而且操作容易。一般的透通模式装置，容易安装于任何网络架构底下，且不需要改变既有的网络设定。

Transport （传输模式）

IPsec 封装机制的一种，传输模式即是所谓的 Host-to-Host 的封装机制，亦即由联机两端主机对其交换的 IP 封包以前段所述的 AH 或（及）ESP 做安全保护，两通讯主机皆须实作有 IPsec。

Trojan （特洛伊木马，Trojan Horse）

顾名思义，特洛伊木马是一种看似无害其实会隐藏起来在计算机内部作怪的程序。它以合法功能的面貌伪装，将病毒特征放在一个外表看起来十分正常的程序当中，等到适当的时机才开始破坏的动作。特洛伊木马一种恶性程序代码 （Malicious code） ，但和病毒 （Virus） 最大的不同是，特洛伊通常不会自我复制，大多用来窃取计算机密码。

UDP （使用者数据流通协议，User Datagram Protocol）

UDP 是传输层通讯方法或通信协议，用于传送短暂需求的少量数据。这个通信协议可提供数据传输量有限的服务，因此不需要验证目的端是否已接收动作的应用程序数据通讯机制。

UID （使用者标识符，User IDentification）

一种码，具有惟一性，可以用来识别一个系统的用户。

URL （统一资源定位器，Uniform Resource Locator）

指明某个体所在位置的标准方式，所谓某个体，通常是指因特网 （Internet） 上的网页，至于其他的个体我们在下面说明。全球信息网 （WWW ） 以 URL 作为网址的格式。在超文件标示语言 （HTML ） 的檔中，利用 URL 来指定超链结（Hyperlink ） 的目标位置，通常这个目标位置就是另一个 HTML 文件 （而且还可能储存在另一台计算机上）。

Virus （病毒）

病毒是一种程序，一种会将自己附加在其他程序里面的软件，当附加程序被执行的时候，病毒程序也跟着启动。病毒具有传播和感染的特性，可能会造成系统损害、删除程序或者数据。病毒通常会附着在可执行文件或启动盘、磁盘，甚至硬盘分割扇区，不过必须附加在其他程序中才能感染另一台计算机，某些病毒也会借着电子邮件 （E-mail ） 感染其他计算机。

VPN （私有虚拟网络，Virtual Private Network）

VPN 是通道 （Tunneling）、加密 （Encryption ）、身分辨认 （Authentication ）、访问控制 （Access Control） 等技术，及经由 Internet、管理式 IP 网络、或网络供货商骨干来传递数据等服务之众多项目的综合体。VPN 能利用公用网络来建立与远程用户、分支办公室及伙伴建立专属连结。如果企业想要有一个安全有保障的广域网环境， VPN 可以透过目前的公众网络，在网络上划分出一条类似私有专线所提供的信道，即所谓的 VPN 的主要组件 — Tunneling，企业包括 Internet、企业内因特网、 企业外部网络的用户都可以在通过安全认证后，在这个通道内不受时间与地点限制，享有其所需的网络服务。

Vulnerability （弱点）

系统或应用程序容易被攻击的点。

WAN （Wide Area Networks）

广域网是能在广大地理区域传送数据的计算机网络，它是由一些透过电信服务连接的局域网络组成。与局域网络不同点在于，它们使用的规约不相同，传输速率比局域网络低。

Worm （计算机蠕虫）

计算机蠕虫也可说是计算机病毒的一种，与病毒不同的是，蠕虫不会感染寄生在其他档案。蠕虫的主要特性是会自我复制并主动散播到网络系统上的其他计算机里面。就像虫一样在网络系统里面到处爬窜，所以称为「蠕虫」。

WWW （World Wide Web ）

因特网的通称。

附錄 F
索引

三划

工具栏 36

四划

内容窗口 36

五划

功能树形图 36

八划

状态栏 37

十划

高可用性 165

十一划

专案树形图 36

十四划

图示 37